(19) **KOREAN INTELLECTUAL PROPERTY OFFICE**

KOREAN PATENT ABSTRACTS

(11)Publication number: **1020000014231 A**

(43)Date of publication of application: **06.03.2000**

(21)Application number: **1019980033521**

(22)Date of filing: **18.08.1998**

(30)Priority: **..**

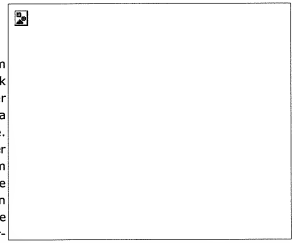
(51)Int. Cl **G06F 17/60**

(71)Applicant: **KOREA ELECTRONICS & TELECOMMUNICATIONS RESEARCH INSTITUTE**

(72)Inventor: **HWANG, SEONG UN**

(54) **OFF-LINE ELECTRONIC TRANSACTION SYSTEM AND ELECTRONIC COMMERCIAL TRANSACTION METHOD USING THE SAME**

(57) Abstract:



PURPOSE: An off-line electronic transaction system is provided to trace a duplicate user utilizing a bank device, assure anonymity and privacy of a legal user device, and enable the bank device to perform a conditional trace by a certificate office device. CONSTITUTION: The system comprises a user device connected to the system to perform electronic commercial transaction, a certificate office device issuing an anonymous certificate to an open key transmitted from the user device, a shop device counting a sole challenger value and supplying user-required product or service to the user device, and a bank device issuing electronic money and increasing the same money as the electronic money in an account of the shop device by receiving the electronic money from the shop device.

Legal Status

Date of request for an examination (19980818)

Notification date of refusal decision (00000000)

Final disposal of an application (registration)
Date of final disposal of an application (20020715)
Patent registration number (1003584260000)
Date of registration (20021014)
Number of opposition against the grant of a patent ( )
Date of opposition against the grant of a patent (00000000)
Number of trial against decision to refuse (2001101002923)
Date of requesting trial against decision to refuse (20010830)
Date of extinction of right ( )

(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl. [6]
G06F 17/60

(45) 공고일자 2003년01월29일
(11) 등록번호 10 -0358426
(24) 등록일자 2002년10월14일

(21) 출원번호 10 -1998 -0033521
(22) 출원일자 1998년08월18일

(65) 공개번호 특2000 -0014231
(43) 공개일자 2000년03월06일

(73) 특허권자 한국전자통신연구원
대전 유성구 가정동 161번지

(72) 발명자 황성운
충청북도 청주시 흥덕구 사직동 215 -1 사직연립 나동 307호

(74) 대리인 김명섭
이화익
권태복

심사관 : 이은철

(54) 전자현금거래방법

요약

본 발명은 오프라인 전자 거래 시스템을 이용한 전자 현금 거래 방법에 관한 것으로서, 전자 화폐의 인출, 지불, 결제 과정이 간단하며 특히 인출 단계에서 사용자 장치에게 부과되는 계산량이 작고 이 또한 대부분 사전 계산 가능하다는 점에서 효율적이다. 또한, 본 전자 화폐는 위조 불가, 익명성, 이중 사용 탐지, 누명 불가 등 전자 상거래에 필수 불가결한 요구 조건들을 모두 만족시킴으로써 인터넷 상에서 사용자들이 안심하고 사용할 수 있도록 함으로써, 효율성이 중시되는 소액권 전자 거래 시스템에서부터 안전성이 더 중시되는 고액권의 전자 거래 시스템에 이르기까지 범용적으로 사용될 수 있도록 한 것이다.

대표도

도 1

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 전자 현금 거래 방법에 적용되는 오프라인 전자 거래 시스템에 대한 연결 구성을 나타낸 도면.

도 2는 본 발명에 따른 전자 현금 거래 방법에 의한 사용자 장치의 인증 과정에 대한 절차를 나타낸 도면.

도 3은 본 발명에 따른 전자 현금 거래 방법에 의한 계좌 개설 과정에 대한 절차를 나타낸 도면.

도 4는 본 발명에 따른 전자 현금 거래 방법에 의한 전자 화폐 인출 과정에 대한 절차를 나타낸 도면.

도 5는 본 발명에 따른 전자 현금 거래 방법에 의한 전자 화폐 지불 과정에 대한 절차를 나타낸 도면.

도 6은 본 발명에 따른 전자 현금 거래 방법에 의한 전자 화폐 결제 과정에 대한 절차를 나타낸 도면.

도 7은 본 발명에 따른 전자 현금 거래 방법에 의한 전자 화폐의 분할 지불 과정에 대한 절차를 나타낸 도면.

도 8은 본 발명에 따른 전자 현금 거래 방법에 의한 전자 화폐의 전이 과정에 대한 절차를 나타낸 도면.

도 9는 본 발명에 따른 전자 현금 거래 방법에 의해 전이된 전자 화폐의 지불 과정에 대한 절차를 나타낸 도면.

< 도면의 주요부분에 대한 부호의 설명 >

100 : 은행 장치 200 : 제1 사용자 장치

300 : 제 2 사용자 장치 400 : 상점 장치

500 : 인증 기관 장치

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 원격 통신 시스템 또는 스마트 카드를 이용하는 암호학적으로 안전하고 효율적인 전자 현금 거래 방법에 관한 것으로서, 특히, 전자 상거래시 사용되는 전자 화폐가 사용자 익명성에 의해 추적이 불가능하고, 다른 사용자에게로 이전할 수 있으며, 잔돈으로 분할 가능하고 동일 화폐를 이중 사용하는 것은 방지할 수 있도록 한 전자 현금 거래 방법에 관한 것이다.

정보 시대의 도래와 함께 세계는 점점 더 네트웍 통신에 의존하고 있으며, 이를 위한 컴퓨터 기반 기술은 정보를 접근, 저장, 배분하는데 지대한 영향을 미치고 있는데, 이러한 기술들 중에 대표적인 것이 바로 통신로 상에서 전자 정보를 교환함으로써 금융 거래를 수행하는 전자 상거래이다.

그러나, 이러한 전자 상거래의 경우, 인터넷과 같은 개방형 네트웍에서는 송수신되는 메시지가 불법 도청되거나 변조됨으로써, 지불자의 프라이버시 침해 또는 금전적인 손실 등 보안 문제가 전자 상거래의 걸림돌로 대두되고 있으며, 또한, 현실적인 측면에서 볼 때, 상기 전자 상거래를 많은 사람이 이용하도록 하기 위해서는 이러한 전자 상거래를 이용함으로써 우리가 지불하는 시스템 비용이 거래 금액에 비해 훨씬 작고 경제적이어야 한다. 따라서, 전자 상거래를 활성화시키기 위해서는 안전하고 효율적인 전자 거래 시스템이 필요하다.

이러한 전자 거래 시스템은 전자 수표, 직불 카드, 신용 카드, 가치 저장 카프(stored value cards) 등의 형태로 출현하고 있으며, 본 발명에서 다루는 전자 거래 시스템은 바로 전자 화폐(electronic cash)에 관한 것으로서, 전자 화폐는

말 그대로 현실 세계에서 통용되고 있는 화폐를 모델로 하여 전자적으로 구현한 것이라 할 수 있다. 이 때, 실세계 화폐는 휴대 가능하고 쉽게 인식할 수 있으며, 이전이 가능하고 잔돈으로 분할 가능하며, 추적이 불가능하고 익명성을 갖추고 있으므로, 전자 화폐 설계시 전자 화폐가 상기와 같은 실세계 화폐의 특성을 가져야 한다. 특히, 이중에서도, 전자 화폐 설계자들이 가장 초점을 두고 있는 특성이 바로 지불 불추적성 (untracibility)과 사용자 익명성(anonymity)이다.

즉, 은행 장치가 누구의 돈이 어디에 쓰였는지 알아낼 수 없도록 지불자 익명성 및 지불 불추적성을 제공하기 위해서는, 은행 장치가 특정 인출 트랜잭션을 특정 예치로 연결시킬 수 없어야 하는데 이것은 온넉 서명 (blind signature, D. Chaum. " Blind signatures for untraceable payments" , the Proceedings of Crypto '88, pp. 199 -203. 1983) 이라는 특별한 종류의 전자 서명을 사용함으로써 가능하다.

또한, 상기 전자 화폐는 디지털 데이터 형태이므로, 동일 화폐를 쉽게 복사하여 여러번 사용할 수 있는데, 이러한 동전의 이중 사용을 막기 위해 온라인 거래 시스템에서는 사용자가 그 전자 화폐를 지불할 때마다 은행이 개입하여 상기 전자 화폐를 확인함으로써 사용자의 이중 사용을 사전에 방지할 수 있으나, 오프라인 방식의 거래 시스템에서는 사용자가 전자 화폐를 상점에 사용할 때 은행이 개입하지 않기 때문에 온라인 거래 시스템에서처럼 전자 화폐의 이중 사용에 대하여, 사전 방지가 쉽지 않다. 다만, 사용자가 사용한 화폐가 상점으로부터 은행에 예치된 후 그 화폐를 은행에 보관할 때, 은행에 저장된 데이터베이스와 비교함으로써 화폐의 이중 사용 여부를 알 수 있다. 즉, 사후에 추적할 수 있을 뿐이다.

이러한 단점을 보완하기 위해, 최근에는 사용자의 지불 장치 내에 은행이 발행하는 물리적 안전 장치(tamper -resistant device)로서, 관찰자(observer)라 불리는 장치를 장착함으로써 화폐의 이중 사용을 사전에 방지하는 방법을 사용하고 있는데, 이 방법에서는 상기 관찰자의 협조가 있어야만 지불이 성공적으로 이루어지게 된다.

발명이 이루고자 하는 기술적 과제

따라서 본 발명의 목적은, 전자 상거래 시 사용되는 전자 화폐가 사용자 익명성에 의해 추적이 불가능하고, 다른 사용자에게로 이전할 수 있으며, 잔돈으로 분할 가능하고 동일 화폐를 이중 사용하는 것을 방지할 수 있도록 한 전자 현금 거래 방법을 제공하는데 있다.

발명의 구성 및 작용

상기한 목적을 달성하기 위한 본 발명의 전자 현금 거래 방법의 일 측면에 따르면, 사용자 장치가 은행 장치와 별개인 인증기관 장치로부터 인증서를 발급 받는 인증서 발급 과정; 사용자 장치가 상기 인증서를 사용하여 자신의 신분을 은행 장치에 노출시키지 않고 은행 장치에 자신의 계좌를 개설하는 계좌 개설 과정; 사용자 장치가 상기 개설된 계좌로부터 은행 장치의 서명이 부여된 전자 현금을 인출하는 전자 현금 인출 과정; 상기 사용자 장치가 은행 장치와 오프라인 상태에서 인증서 및 전자 현금을 사용하여 특정 상거래에 대한 지불을 수행하는 전자 현금 지불 과정으로 이루어지되, 상기 인증서 발급 과정은, 사용자 장치가 이산 대수형 서명 체계를 이용하여 사용자의 비밀키 및 공개키를 생성하는 단계; 사용자 장치가 인증기관 장치에게 자신의 신원을 입증하면서 상기 사용자 장치의 공개키를 전송하는 단계; 인증기관 장치가 인증기관 장치의 비밀키, 사용자 장치의 공개키 및 인증 기관 장치의 신원 정보를 사용하여 상기 사용자 장치의 공개키에 대한 인증서를 생성하는 단계; 상기 인증기관 장치가 상기 인증서를 사용자 장치에 전송하는 단계 및 사용자 장치가 상기 인증기관 장치의 공개키, 인증기관 장치의 신원 정보 및 사용자 장치의 공개키를 사용하여 상기 인증서의 유효성을 확인하는 단계로 이루어지고, 상기 인증서를 생성하는 단계에서, 상기 인증서의 생성은 아래의 수학식을 이용하는 것이다.

$$Cert_u = h(ID_{CA} \| p_u)^{d_{CA}} \bmod n_{CA}$$

여기서, 상기 $Cert_u$는 인증서, ID_{CA} 는 인증기관 장치의 신원 정보, p_u는 사용자 장치의 공개키, d_{CA} 는 인증기관 장치의 비밀키, n_{CA} 는 인증기관 장치의 공개 모듈러스, h는 일방향 함수이다.

상기 공개키를 생성하는 단계에서 공개키의 생성과, 인증서의 유효성을 확인하는 단계에서, 유효성의 확인은 아래의 수학식을 이용할 수 있다.

$$p_u = g^{-S_U} \bmod p$$

$$Cert_u^{e_{CA}} \bmod n_{CA} = h(ID_{CA} \| p_u)$$

여기서, P_u는 사용자 장치의 공개키, S_u는 사용자 장치의 비밀키, g는 Z^*_p의 부분군 G_q의 생성자이다. 또한, 상기 Certu는 인증서, ID_{CA} 는 인증기관 장치의 신원 정보, p_u는 사용자 장치의 공개키, e_{CA} 는 인증기관 장치의 공개키, n_{CA} 는 인증기관 장지의 공개 모듈러스, h는 일방향 함수이다.

또한, 본 발명에 따른 전자 현금 거래 방법의 다른 측면에 따르면, 사용자 장치가 은행 장치와 별개인 인증기관 장치로부터 인증서를 발급 받는 인증서 발급 과정; 사용자 장치가 상기 인증서를 사용하여 자신의 신분을 은행 장치에 노출시키지 않고 은행 장치에 자신의 계좌를 개설 과정; 사용자 장치가 상기 개설된 계좌로부터 은행 장치의 서명이 부여된 전자 현금을 인출하는 전자 현금 인출 과정; 상기 사용자 장치가 은행 장치와 오프라인 상태에서 인증서 및 전자 현금을 사용하여 특정 상기레에 대한 지불을 수행하는 전자 현금 지불 과정으로 이루어지되, 상기 인증서 발급 과정은, 사용자 장치가 이산 대수형 서명 체계를 이용하여 사용자의 비밀 키 및 공개키를 생성하는 단계; 사용자 장치가 인증기관 장치에게 자신의 신원을 입증하면서 상기 사용자 장치의 공개키를 전송하는 단계; 인증기관 장치가 인증기관 장치의 비밀키, 사용자 장치의 공개키 및 인증기관 장치의 신원 정보를 사용하여 상기 사용자 장치의 공개키에 대한 인증서를 생성하는 단계; 상기 인증기관 장치가 상기 인증서를 사용자 장치에 전송하는 단계 및 사용자 장치가 상기 인증기관 장치의 공개키, 인증기관 장치의 신원 정보 및 사용자 장치의 공개키를 사용하여 상기 인증서의 유효성을 확인하는 단계로 이루어지고, 상기 사용자 장치 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계에서 공개키 및 인증서의 확인은 아래의 수학식을 이용하는 것이다.

$$Cert_u^{e_{CA}} \bmod n_{CA} = h(ID_{CA} \| p_u)$$

여기서, 상기 $Cert_u$는 인증서, ID_{CA} 는 인증기관 장치의 신원 정보, p_u는 사용자 장치의 공개키, e_{CA} 는 인증기관 장치의 공개키, n_{CA} 는 인증기관 장치의 공개 모듈러스, h는 일방향 함수이다.

본 발명에 따른 전자 현금 거래 방법의 또 다른 측면에 따르면, 사용자 장치가 은행 장치와 별개인 인증기관 장치로부터 인증서를 발급 받는 인증서 발급 과정; 사용자 장치가 상기 인증서를 사용하여 자신의 신분을 은행 장치에 노출시키지 않고 은행 장치에 자신의 계좌를 개설하는 계좌 개설 과정; 사용자 장치가 상기 개설된 계좌로부터 은행 장치의 서명이 부여된 전자 현금을 인출하는 전자 현금 인출 과정; 상기 사용자 장치가 은행 장치와 오프라인 상태에서 인증서 및 전자 현금을 사용하여 특정 상거래에 대한 지불을 수행하는 전자 현금 지불 과정으로 이루어지되, 상기 전자 현금 인출 과정은, 상기 사용자 장치가 전자 현금 난수를 발생하고 상기 전자 현금 난수에 대한 이미지를 생성하는 단계; 상기 사용자 장치가 전자 현금 인출을 위한 메시지를 생성하고 상기 메시지를 은닉하는 단계; 상기 사용자 장치가 상기 메시지에 관한 사용자 장치의 서명을 생성하는 단계; 상기 사용자 장치가 상기 메시지, 상기 사용자 장치의 서명, 사용자 장치의 공개키 및 그에 상응하는 인증서를 전송하는 단계; 상기 은행 장치에서 사용자 장치의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계; 상기 은행 장치가 상기 사용자 장치 서명의 유효성을 확인하는 단계; 상기 사용자 장치의 공개키 및 그에 상응하는 인증서 그리고 상기 서명이 모두 유효하면 상기 은행 장치가 상기 은닉된 메시지에 은행 장치의 서명을 하는 단계; 상기 은행 장치가 상기 은행 장치에 서명된 메시지를 상기 사용자 장치로 전송하는 단계; 상기 사용자 장치가 상기 은행 장치로부터 은행 장치에 서명된 메시지를 얻고, 얻은 메시지와 상기 발생된 난수를 전자 현금으로 저장하는 단계로 이루어지고, 상기 사용자 장치 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계에서 공개키 및 인증서의 확인은 아래의 수학식을 이용하는 것이다. 상기 전자 현금 난수에 대한 이미지를 생성하는 단계에서의 난수는, {1, ... q}에서 랜덤하게 선택된 어느 하나이고, 상기 난수의 이미지는 $r' = g^{r} \bmod p$ 따라 생성될 수 있다. 여기서, r은 난수, r'는 이미지, g는 Z^{*}_{p}의 G(q)의 생성자이고, q는 G(q)의 위수이다.

또한, 본 발명의 전자 현금 거래 방법의 또 다른 측면에 따르면, 사용자 장치가 은행 장치와 별개인 인증기관 장치로부터 인증서를 발급 받는 인증서 발급 과정; 사용자 장치가 상기 인증서를 사용하여 자신의 신분을 은행 장치에 노출시키지 않고 은행 장치에 자신의 계좌를 개설하는 계좌 개설 과정; 사용자 장치가 상기 개설된 계좌로부터 은행 장치의 서명이 부여된 전자 현금을 인출하는 전자 현금 인출 과정; 상기 사용자 장치가 은행 장치와 오프라인 상태에서 인증서 및 전자 현금을 사용하여 특정 상거래에 대한 지불을 수행하는 전자 현금 지불 과정으로 이루어지되, 상기 사용자 장치를 지불자라고 하고, 그의 상거래 상대방을 피지불자라고 할때, 상기 전자 현금 지불 과정은, 상기 지불자가 전자 현금 메시지, 그 자신의 공개키 및 그에 상응하는 인증서를 피지불자에게 전송하는 단계, 피지불자는 상기 지불자의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계; 상기 피지불자의 은행 계좌 번호 및 거래 시간을 상기 지불자에게 전송하는 단계; 상기 피지불자가 상기 전자 현금 메시지, 그에 은행 계좌 번호 및 상기 거래 시간에 근거하는 챌린저값을 산출하는 단계; 상기 지불자가 상기 전자 현금 메시지, 상기 피지불자의 은행 계좌 번호 및 상기 거래 시간에 근거하는 챌린저값을 산출하는 단계; 상기 지불자가 상기 전자 현금 메시지. 상기 피지불자의 은행 계좌 번호 및 상기 거래 시간에 근거하여 챌린저값을 산출하는 단계; 상기 지불자가 상기 전자 현금에 관련된 난수, 상기 챌린저값, 지불자의 비밀키를 이용하여 상기 챌린저값에 대한 반응값을 생성하는 단계; 상기 지불자가 상기 반응값을 상기 지불자에게 전송하는 단계; 상기 피지불자가 상기 반응값의 유효성을 확인하는 단계; 상기 반응값이 유효하면, 상기 피지불자가 상기 전자 현금을 받아들이는 단계를 포함하고, 여기서, 상기 피지불자가 지불자의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계에서의 유효성 확인은 아래의 수학식을 이용할 수 있다.

$$Cert_{u}^{e_{CA}} \bmod n_{CA} = h(ID_{CA} \| p_{u})$$

여기서, 상기 $Cert_u$는 인증서, ID_{CA} 는 인증기관 장치의 신원 정보, p_u는 사용자 장치의 공개키, e_{CA} 는 인증기관 장치의 공개키, n_{CA} 는 인증기관 장치의 공개 모듈러스, h는 일방향 함수이다.

본 발명에 따른 전자 현금 거래 방법의 또 다른 측면에 따르면, 사용자 장치가 은행 장치와 별개인 인증기관 장치로부터 인증서를 발급 받는 인증서 발급 과정; 사용자 장치가 상기 인증서를 사용하여 자신의 신분을 은행 장치에 노출시키지 않고 은행 장치에 자신의 계좌를 개설 과정; 사용자 장치가 상기 개설된 계좌로부터 은행 장치의 서명이 부여된 전자 현금을 인출하는 전자 현금 인출 과정; 상기 사용자 장치가 은행 장치와 오프라인 상태에서 인증서 및 전자 현금을 사용하여 특정 상기래에 대한 지불을 수행하는 전자 현금 지불 과정으로 이루어지되, 상기 전자 현금 지불 과정은, 지불자가 지급 현금 난수 r_1 및 잔여 전자 현금 난수 r_2를 선택하는 단계; 상기 지불자가 상기 지급 전자 현금 난수 및 잔여 현금 난수의 이미지들 r'_1, r'_2를 생성하는 단계; 상기 지불자가 상기 전자 현금 메시지 c, 상기 전자 현금 난수의 이미지 r', 상기 전자 현금의 금액 A, 지급 전자 현금 난수의 이미지 r'_1, 지급 전자 현금의 금액 A_1 및 잔여 전자 현금 난수의 이미지 r'_2에 근거하여 전자 현금 메시지 서명 d를 산출하고, 이에 상응하는 전자 현금 메시지 서명 반응값 z를 상기 전자 현금 메시지 서명 d, 지불자의 비밀키 Su 및 상기 전자 현금 난수 r을 사용하여 생성하는 단계; 상기 지불자가 피지불자에게 전자 현금 메시지 c, 상기 전자 현금 난수의 이미지 r', 상기 전자 현금의 금액 A, 지급 전자 현금 난수의 이미지 $r'1$, 지급 전자 현금의 금액 A_1, 잔여 전자 현금 난수의 이미지 r'_2, 상기 전자 현금 메시지 서명 d, 지불자의 공개키 P u 및 그에 상응하는 인증서 $Cert_U$를 피지불자에게 전송하는 단계; 피지불자는 상기 지불자의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계; 상기 피지불자의 은행 계좌 번호 및 거래 시간을 상기 지불자에게 전송는 단계; 상기 피지불자가 지급 전자 현금 난수의 이미지 r'_1, 지급 전자 현금의 금액A_1, 그의 은행 계좌번호 As 및 거래 시간 time에 근거하여 챌린저값 d_1을 산출하는 단계; 상기 지불자가 상기 지급 전자 현금 난수의 이미지 r'_1, 지급 전자 현금의 금액 A_1, 상기 피지불자의 은행 계좌번호 As 및 상기 거래 시간 time, 지불자의 비밀키 S_U, 전자 현금 난수 r에 근거하여 상기 챌린저값에 대한 반응값 z_1을 생성하는 단계; 상기 지불자가 상기 반응값을 상기 피지불자에게 전송하는 단계; 상기 피지불자가 상기 챌린저값에 대한 반응값 z1의 유효성을 확인하는 단계; 상기 반응값이 유효하면, 상기 피지불자가 상기 전자 현금을 받아들이는 단계를 포함할 수 있다.

이하, 본 발명에 따른 전자 현금 거래 방법에 대한 바람직한 실시예에 대하여 첨부한 도면을 참조하여 상세하게 살피보기로 한다.

도 1은 본 발명에 따른 전자 현금 거래 방법에 적용되는 오프라인 전자 거래 시스템에 대한 구성도로서, 도 1을 참조하면, 본 발명의 전자 거래 시스템은 상기 전자 거래 시스템에 접속하여 전자 상거래를 수행하는 사용자 장치(200, 300)와, 상기 사용자 장치(200 또는 300)가 자신의 신원을 입증하며 공개키를 전송하여 인증서를 요구할 경우, 그 사용자 장치의 신원을 확인한 후 사용자 장치가 전송한 공개키에 대한 익명의 인증서를 발행하는 인증기관 장치(500)와, 상기 사용자 장치(200 또는 300)로부터 전자 화폐와 그 사용자 장치(200 또는 300)에 대한 공개키 및 익명의 인증서를 받아 각 거래에 대해 유일한 챌린저(challenger)값을 계산하고 그 챌린저 값에 의해 상기 전자 화폐를 확인한 후, 사용자 장치(200 또는 300)가 요구한 상품이나 서비스를 상기 사용자 장치(200 또는 300)로 제공하는 상점 장치(400)와, 상기 사용자 장치(200 또는 300)의 공개키 및 대응하는 인증서만으로 그 사용자 장치(200 또는 300)에게 익명의 계좌를 개설해주어 상기 사용자 장치(200 또는 300)의 요구에 따라 전자 화폐를 발행하고, 상기 상점 장치(400)로부터 전자 화폐를 예치 받아 상기 상점 장치(400)의 계좌에 전자 화폐와 동일한 금액을 증가시키는 은행 장치(100)들이 원격 통신 네트웍을 통하여 상호 연결되어 있다. 이 때, 상기 사용자 장치(200 또는 300)는 원격통신 네트웍을 통하지 않고 스마트 카드를 가지고 직접적으로 상점 장치(400)에 지불할 수도 있다.

이 때, 상기 사용자 장치(200 또는 300)는 난수 발생 및 지수 연산의 암호학적 연산 능력을 갖춘 IC 카드 또는 그에 준하는 계산 장치이고, 상기 상점 장치(400)는 IC 카드 단말기 또는 상기 IC 카드에 준하는 계산 장치이며, 상기 사용자 장치(200 또는 300)는 상기 은행 장치(100)로부터 전자 화폐를 인출하고자 하는 경우, 이산 대수형 서명(∑)을 생성하여, 공개키 및 익명의 인증서와 함께 상기 은행 장치(100)로 전송한다.

한편, 상기 인증기관 장치(500)는 상기 사용자로부터 인증서의 발행 요구가 있을 경우, 은닉 서명을 이용하여 익명의 인증서를 발행하며, 상기 사용자 장치(200 또는 300)의 신원 정보와 사용자로부터 전송된 공개키 및 발행한 익명의 인증서를 저장하고 있다가, 사용자 장치가 화폐를 이중 사용하는 등 공정한 전자 상거래를 수행하지 않은 경우, 그 사용자 장치를 추적하는 데에 사용한다.

또한, 상기 은행 장치(100)는 상기 사용자로부터 전자 화폐 인출의 요구가 있을 경우, 발행하고자 하는 전자 화폐가 위조 불가능하도록 하기 위해 그 전자 화폐 후보에 서명을 하여 사용자 장치(200 또는 300)로 전송한다.

이러한 구성을 갖는 본 발명의 전자 거래 시스템의 동작을 간략하게 살펴보면, 사용자 장치(200 또는 300)가 그의 공개키를 등록할 때 상기 인증기관 장치(500)는 상기 사용자 장치(200 또는 300)에게 익명의 인증서를 발행하고, 상기 은행 장치(100)는 상기 사용자 장치(200 또는 300)의 요청에 따라 어떤 액면가의 전자 화폐를 발행하며, 상기 사용자 장치(200 또는 300)는 그 전자 화폐의 액면가에 다다를 때까지 상기 상점 장치(400)에서 그 전자 화폐를 여러 번 분할해서 사용할 수 있다. 그러면, 상기 상점 장치(400)는 상기 사용자 장치(200 또는 300)에 의해 지불된 전자 화폐를 상기 은행 장치(100)에 예치한다.

이러한 본 발명의 전자 거래 시스템에 의한 전자 상거래 방법은 인증서 발급 절차, 계좌 개설 절차, 전자 현금 인출 절차, 전자 현금 지불 절차 및 전자 현금 예치 절차를 포함한다.

인증서 발급 절차는, 상기 사용자 장치가 자신의 신원을 입증하며 공개키를 전송하여 인증서를 요구한 경우, 상기 인증기관 장치가 그 사용자 장치의 신원을 확인한 후, 사용자 장치가 전송한 공개키에 대한 익명의 인증서를 발행한다.

계좌 개설 절차는, 상기 사용자 장치가 상기 은행 장치에게 익명의 인증서와 자신의 공개키를 전송하여 익명의 계좌 개설을 요구하면, 상기 은행 장치는 그 공개키가 상기 인증기관 장치에 등록되었는지를 확인한 후, 그 사용자 장치에게 익명의 계좌를 개설하여 준다.

전자 현금 인출 절차는, 상기 사용자 장치가 상기 은행 장치로 전자 현금 인출 요구를 하면 은행 장치는 사용자 장치를 확인한다. 사용자 장치의 인출 요구가 정당하면, 은행 장치는 은닉된 유효 전자 현금을 사용자 장치에게 발생하고 발행된 전자 현금의 가치를 사용자 장치의 계좌에서 감소시킨다.

전자 현금 지불 절차는 상기 사용자 장치가 전자 현금과, 자신의 공개키와, 익명의 인증서를 상점 장치에 전송하고, 원하는 상품이나 서비스를 선택하면, 상기 상점 장치가 그 전자 현금의 유효성을 확인한 후, 상기 선택된 상품이나 서비스를 그 사용자에게 제공한다.

전자 현금 예치 절차는 상기 상점 장치가 사용자로부터 받은 전자 현금을 은행 장치에 예치하기 위해, 상기 전자 현금 및 그 전자 현금의 사용자에 대한 공개키와 익명의 인증서를 은행 장치로 전송한다. 은행 장치는 상기 상점 장치로부터 받은 정보에 의해 공개키 및 전자 현금의 유효성 및 이중 사용 여부를 확인한 후, 예치 요구가 정당한 것이면, 그 전자 현금을 상기 상점 장치의 계좌에 예치시키는 것이다.

본 발명에 따른 전자 거래 방법은 또한, 전자 현금 분할 지불 절차, 전자 현금 전이 절차 및 전이된 전자 현금 지불 절차를 포함한다.

전자 현금 분할 지불 절차에서 사용자 장치는 전자 현금을 복수의 전자 현금으로 나누되, 복수의 전자 현금들의 가치의 합은 원 전자 현금의 가치와 동일하게 되도록 복수의 전자 현금으로 분할하여 그 중 하나의 전자 현금을 상점 장치로 지불한다.

전이된 전자 현금 지불 절차는 다른 사용자 장치로부터 전이된 전자 현금을 상점 장치에게 지불하기 위한 것이다.

이 때, 상기 은행 장치(100)와 인증기관 장치(500)는 다음과 같이 RSA 기법에 의해 초기화되며, 상기 은행 장치(100)의 공개키/비밀키 쌍은 (e_B, n_B) /d_B이고, 상기 인증기관 장치(500)의 공개키/비밀키 쌍은 (e_{CA}, n_{CA}) /d_{CA} 로서, 그 각각은 $e_B \cdot d_B = 1 \bmod \phi(n_B)$ 및 $e_{CA} \cdot d_{CA} = 1 \bmod \phi(n_{CA})$ 을 만족하는 것을 특징으로 한다. 상기 은행 장치(100)는 다양한 금액의 전자 화폐를 발행하기 의해 금액별로 서로 다른 공개키/비밀키 쌍을 준비한다. 단 ϕ 는 Euler totient 함수이다. 한편, h는 다항식 시간 충돌회피성 일방향 함수를 나타내며, 위에서 공개키는 모든 사람들에게 알려지는 부분이다. 은행 장치는 전자 현금의 서로 다른 값을 발생하는데 몇몇의 공개키/비밀키의 쌍을 준비한다.

이러한 본 발명의 전자 현금 거래 방법을 도 2 내지 도 9를 참조하여 상세히 설명하면 다음과 같다.

도 2는 본 발명의 전자 현금 거래 방법에 의한 사용자 장치의 인증 과정에 대한 절차도로서, 도 2를 참조하면, 상기 인증기관 장치(500)에서 사용자 장치(200 또는 300)에게 익명의 인증서를 발행하는 과정은 먼저, 사용자 장치(200)가 상기 이산 대수형 서명 체계를 이용하여 자신의 비밀키(S_u) 및 공개키(p_u)를 생성(S201)한 후, 상기 인증기관 장치(500)에게 자신의 공개키(p_u)를 전송(S202)하면, 상기 인증기관 장치(500)가 상기 공개키(p_u)에 대한 익명의 인증서($Cert_u$)를 생성(S203)하여 그 사용자 장치(200)에게 전송(S204)하고, 상기 사용자 장치(200)가 그 인증서($Cert_u$)를 확인(S205)하는 과정으로 구성된다.

이 때, 상기 사용자 장치(200)는 자신의 공개키/비밀키 쌍을 생성하기 위해, Schnorr (C.P.Schnorr, " Efficient Signature Generation By Smart Cards" , J.of Cryptology, 4 -3, pp. 161 -174. 1991), DSA (Digital Signature Algorithm), KDSA (Korean Digital Signature Algorithm) 등과 같은 이산대수형 서명 체계를 선택하며, 집합 {1, ..., q}에서 랜덤하게 비밀키(S_U)를 선택하고 그로부터 공개키($p_u = g^{-SU} \bmod p$)를 계산하며, 인증기관 장치(500)에게 상기 공개키(p_u)를 보낼 때, 자신의 신원을 입증하는 과정을 동시에 수행한다. 이 때, p와 q는 각각 512비트, 140비트 이상의 크기를 가지는 소수로서 q는 p -1을 나눈다. g는 Z^*_p의 부분군 Gq의 생성자(generator)이다.

한편, 상기 인증기관 장치(500)는 사용자 장치(200)의 신원을 확인한 후, 수신한 공개키(p_u)에 대한 인증서($Cert_u = h(ID_{CA} \, IIp_u)^{dCA} \bmod n_{CA}$)를 사용자 장치(200)에게 발급하며, 상기 공개키(pu)와 인증서($Cert_u = h(ID_{CA} \, IIp_u)^{dCA} \bmod n_{CA}$)를 사용자 장치(200)의 신원 정보와 함께 저장하여, 상기 전자 거래 시스템에서 사용자 장치(200)의 신원을 확인할 필요가 있을 때 사용한다. 여기서 ID_{CA}는 인증기관장치(500)의 신원 정보를 나타낸다. 한편, 사용자 장치(200)는 인증기관 장치(500)로부터 받은 인증서를 체크($[Cert_u]^{eCA} \bmod n_{CA} = h(ID_{CA} \, IIp_u)$) 한다.

이 때, 상기 인증기관 장치(500)에서 사용자 장치(200)로 발급되는 인증서는 사용자의 신원과 공개키 사이의 연결 관계를 수립하는 역할을 한다. 즉, 해당 공개키가 인증기관 장치(500)에 등록되어 있음을 의미한다. 그러나, 보통의 인증서와는 달리, 이 연결 관계는 모든 사람들로부터 비밀로 유지되게 함으로써, 인증기관을 제외한 어느 누구도 공개키 또는 인증서로부터 사용자(소유자)의 신원을 알아낼 수 없다.

도 3은 본 발명의 전자 현금 거래 방법에 의한 계좌 개설 과정에 대한 절차도로서, 도 3은 참조하면 은행 장치(100)에서 사용자 장치(200)로 계좌를 개설하는 과정은 사용자 장치(200)가 은행 장치(100)에게 자신의 신분을 밝히지 않으면서 자신의 공개키(P_u) 및 대응하는 인증서($Cert_u$)를 전송(S301)하면, 상기 은행 장치(100)는 인증서($Cert_u$)를 확인($[Cert_u]^{eCA} \bmod n_{CA} = h(ID_{CA} \, IIp_u)$?) (S302)하여 상기 공개키(P_u)가 인증기관 장치(500)에 등록되었는지를 확인하여, 확인이 통과되면 그 공개키(P_u)에 대한 계좌를 개설(S303)한다. 이 과정에서는 사용자 장치(200)는 은행 장치(100)로부터 전자 화폐를 인출할 수 있는 익명의 계좌를 얻는다.

도 4는 본 발명의 전자 현금 거래 방법에 의한 전자 화폐 인출 과정에 대한 절차도로서, 도 4를 참조하면, 본 발명의 전자 화폐 인출 과정은 사용자 장치(200)가 공개키(P_u)에 대응하는 그의 계좌로부터 인출을 원할 때, 상기 사용자 장치(200)는 은행장치(100)와 다음 과정들을 수행한다.

먼저, 사용자 장치(200)는 집합 {1, ..., q}에서 난수(r)를 발생시켜 $r' = g^r \bmod p$를 계산하고, 전자 화폐 후보($c' = h(r' \, IIp_u) \bmod n_B$)를 생성(S401)하고, 그 전자 화폐 후보(c')에 대한 이산 대수형 서명($\sum$)을 생성하여, 상기 전자 화폐 후보(c')와 이산 대수형 서명($\sum$)을 사용자 장치의 공개키(p_u) 및 인증서($Cert_u$)와 함께 은행 장치(100)로 전송(S402)한다.

은행 장치(100)가 상기 인증서($Cert_u^{eCA} \bmod n_{CA} = h(ID_{CA} \, IIp_u)$)를 확인한 다음, 공개키($p_u$)를 가지고 이산 대수형 서명($\sum$)을 확인(S403)한 후, 만약 확인 과정이 통과되면 상기 전자 화폐 후보(c')에 전자 서명된 화폐 $(c = [c']^{dB} \bmod n_B = [h(r' \, IIp_u)]^{dB} \bmod n_B)$를 발행(S404)하여 사용자 장치(200)에 전송(S405)한 후, 상기 사용자 장치(200)의 계좌에서 발행된 전자 화폐의 금액만큼 감소시킨다.

그러면, 상기 사용자 장치(200)는 상기 은행 장치(100)로부터 얻은 상기 전자 화폐(c)의 유효성을 인증한($c^{eB} \bmod n_B = [h(r' \, IIp_u)]$) (S406) 다음, 그 전자 화폐 정보 {c, r}를 저장(S407)한다.

이 때, 상기 사용자 장치(200)는 전자 화폐 생성시 필요한 값들, 예를 들어 상기 난수 (r, r')을 인출 전에 미리 계산(오프라인 사전 계산)해 두었다가 인출 단계에서 사용함으로써, 인출 단계에서 사용자 장치에게 부과되는 계산량을 줄인다.

도 5는 본 발명의 전자 현금 거래 방법에 의한 전자 화폐 지불 과정에 대한 절차도로서, 이 때, 사용자 장치(200)는 주어진 전자 화폐를 분할하지 않고 액면 금액 그대로 사용하는 경우로서, 도 5를 참조하면 사용자 장치(200)가 상점 장치(400)에게 A원의 현금(c)을 지불하고자 할 때 다음 단계들이 수행된다. 즉, 지불자로서 사용자 장치(200)를 나타내고, 피지불자로서 상점 장치(400)를 나타낸 것이다.

먼저, 사용자 장치(200)가 전자 화폐(c), 공개키(P_u), 인증서($Crert_u$)를 상점 장치(400)에 전송(S501)하면, 상기 상점 장치(400)는 인증서($Cert_u = h(ID_{CA}\ IIp_u)$)를 확인(S502)하고, 상기 현금(c), 지불 거래가 발생한 시각(time) 및 상점 장치(400)의 계좌번호(As)를 가지고 각 거래(transaction)에 대하여 유일한 값인 챌린지(challenge)값($d = h(AsIItimeIIc)$)을 계산(S503)한 후 자신의 계좌 번호(As) 및 트랜잭션 발생 시각(time)을 사용자 장치(200)에게 전송(S504)한다.

그러면, 상기 사용자 장치(200)는 상기 상점 장치(400)와 동일하게 챌린지 값($d = h(AsIItimeIIc)$) 및 반응값($z = (t+S_u d) \bmod q$)을 계산(S505)한 후, 이 반응값(z)을 상점 장치(400)로 전송(S506)하고, 상기 상점 장치(400)는 상기 사용자 장치로부터 받은 정보를 가지고 $w = g^{u}\ p^{u} \bmod p$를 계산하고 전자 화폐의 유효성을 확인($c^{eB} \bmod_B = h(wIIp_u)$)(S507)하여, 상기 확인 과정(S507)이 통과되면, 상점 장치(400)는 상기의 전자 화폐를 받아들이고 사용자 장치(200)가 구매 요청한 상품이나 서비스를 제공한다.

도 6은 본 발명의 전자 현금 거래 방법에 의한 전자 화폐 결제 과정에 대한 절차도로서, 도 6을 참조하면, 전자 화폐 결제 과정은 먼저, 네트웍 트래픽이 낮은 적절한 때에 상기 상점 장치(400)가 전자 화폐 및 관련 정보{c, Cert $_u$, p_u, d, time, As, z}를 은행 장치(100)에게 전송(S601)하여 사용자 장치(200)로부터 받은 모든 동전을 은행 장치(100)에 예치하면, 상기 은행 장치(100)는 챌린저값($d = h(AsIItimeIIc)$) 및 $w = g^{z}p_u^{d} \bmod p$를 계산하고 공개키(P_u), 인증서($Cert_u{}^{eCA}\ modn_{CA} = h(ID_{CA}\ IIp_u)$) 및 전자 화폐($c^{eB}\ modn_B = h(wIIp_u)$)를 확인(S662)한 후, 상기 상점 장치(400)로부터 받은 전자 화폐(c)가 자신의 예치 데이터 베이스(DB)에 저장되어 있는지를 알아보기 위해 탐색(S603)한다.

상기 은행 장치(100)의 탐색(S603)결과 상점 장치(400)로부터 받은 전자 화폐(c)가 자신의 예치 데이터베이스(DB)에 저장되어 있지 않으면, 상기 은행 장치(100)는 상점의 계좌에 상기 전자 화폐 금액만큼 증가(S604)시키고 거래 기록을 데이터베이스에 저장하고, 만일, 동일한 동전이 자신의 예치 데이터베이스(DB)에서 발견되면 이는 이중 사용을 의미하므로, 상기 은행 장치(100)는 그 동전을 받아들이지 않고 인증기관 장치(500)의 도움을 받아 이중 사용자 추적을 행한다.

이 때, 상기 이중 사용자 추적은 상기 은행 장치(100)에 의해 동일한 전자 화폐에 사용된 서로 다른 챌린저 값(d, d')과 반응값 $z = (r+S_u d) \bmod q$, $z' = (r+S_u d') \bmod q$로부터 전자 화폐를 이중으로 사용한 사용자 장치의 비밀키($S_u = (z-z') / (d-d') \bmod q$)를 찾아내고, 상기 사용자 장치의 비밀키를 상기 인증기관 장치에 제시함으로써 가능하다.

도 7은 본 발명에 따른 전자 현금 거래 방법에 의한 전자 화폐의 분할 지불 과정에 대한 절차도로서, 사용자 장치(200)는 동전을 임의 금액의 두 부분으로 나누어 사용할 수 있으며, 이 때 두 부분의 금액의 합은 분할 전 전자 화폐의 액면가와 동일해야 하고, 이 프로시저는 수정된 Schnorr서명 체계에 기반한다.

이 때, 상기 사용자 장치(200)는 A원인 전자 화폐 c를 상점에 A_1(이 때, $A_1 < A$) 원을 지불하고자 하며, 동전 c를 각각 A_1, $A - A_1$에 해당하는 동전 c_1, c_2로 분할하여 상점 장치(400)로 지불하고자 하는 경우이다.

도 7을 참조하면, 상기와 같은 전자 화폐 분할 지불 과정은 다음과 같다.

먼저, 사용자 장치(200)가 하나의 동전을 몇 개의 동전들로 분할(S701)하여 관련 정보를 상점 장치(400)에 전송(S702)하면, 상기 상점 장치(400)는 사용자 장치(200)의 인증서($Cert_u{}^{eCA}\ modn_{CA} = h(ID_{CA}\ IIp_u)$) 및 $c^{eB}\ modnB = h(g^{s}p^{t}{}_{u}IIP_u)$를 확인(S703)한 다음 챌린저 값($d1 = h(r_1\ 'IIA_1\ IIAsIItime)$)을 계산(S704)하고 자신의 계좌 번호(As) 및 트랜잭션 발생 시각(time)을 사용자 장치에게 전송(S705)한다.

그러면, 상기 사용자 장치(S706)는 상점 장치와 똑같이 챌린저 값($d_1 = h(r_1 \| ID_A \| ID_B \| Itime)$)을 계산한 후, 동전 속에 포함된 비밀 정보, 상기 사용자의 비밀키 및 챌린저 값으로부터 반응값(response value) ($z_1 = (r' + s_u d_1) \bmod q$)을 계산(S706)하여 그 반응값($z_1$)을 상점 장치(400)로 전송(S707)하여, 상기 상점 장치(400)는 상기 반응값(z_1), 사용자 장치의 공개키(p_u) 및 상기 챌린저 값(d_1)을 이용하여 $w_1 = g^{z_1} p_u^{d_1} \bmod p$를 계산하며, 상기 전자 화폐($c^{eB} \bmod n_B = h(w_1 \| ID_{pu})$)를 확인(S708)한다.

단계 S701에서 사용자 장치(200)는 하나의 동전을 분할하기 위해, 집합 {1, ..., q}에서 임의로 r_1, r_2를 택한 다음 $r_1' = g^{r_1} \bmod p$, $r_2' = g^{r_2} \bmod p$를 각각 계산하여 저장하고, $d = h(cID \| r_1' \| ID_A \| ID_B \| r_2')$와 $z = (r + S_u d) \bmod q$를 계산하는데, 이때, 상기 상점 장치(400) 및 사용자 장치(200)가 계산하는 챌린저 값(d)은 Schnorr 체계를 사용하여 메시지 {c, r, A, r_1, A_1, r_2}에 대한 서명을 생성하는 것으로 생각할 수 있으며, 사용자 장치(200)는 A_1원의 전자 화폐로서 정보 {c, r, A, r_1, A_1, r_2, d, z, p_u, $Cert_u$}를 상점 장치(400)에게 전송한다.($r' = g^r \bmod p$이다.)

요약하면, 지불자(사용자 장치(200))와 지불 받는 사람(상점장치(400))은 상기 거래 결과 발생 기록인 {c, r', A, r_1', A_1, r_2', d, z_1, w_1}를 저장해야 하는데, 상기 지불자의 경우 상기 전자 화폐의 나머지 부분, 즉 A - A_1 금액의 c_2 (r_2')를 지불하기 위해서 거래 기록을 필요로 하며, 지불 받는 사람은 받은 동전을 나중에 지불하거나 은행 장치(100)에 예치할 때 그 거래 기록을 필요로 한다.

한편, 사용자 장치가 자신이 인출한 전자 화폐를 다른 사용자 장치에게로 전이하여, 그 사용자 장치가 전이된 전자 화폐를 상기 상점 장치로 지불하고자 하는 경우, 제1 사용자 장치가 자신의 계좌에 입금된 전자 화폐에 대한 소유권을 제2 사용자 장치에게 이전함으로써, 제1 사용자 장치(200)의 전자 화폐가 제2 사용자 장치(300)에게 전이되도록 하는 전이 단계와, 상기 제 2사용자 장치가 상기 제1 사용자 장치로부터 전이된 전자 화폐를 상점 장치에게 지불하도록 하는 지불 단계를 수행한다. 이 때, 가능한 전이 횟수는 은행이 발행한 빈 동전에 의해 결정되며, 전자 화폐는 전이될 때마다 그 크기가 증가하게 된다.

도 8은 본 발명의 전자 현금 거래 방법에 의한 전자 화폐의 전이 과정에 대한 절차도로서, 상기 전자 화폐 전이 과정을 수행하기 전에 상기 제 1사용자 장치(200)와 제2 사용자 장치(300)는 각각 익명의 인증서($Cert_{u1}$ 와 $Cert_{u2}$)를 갖고 있어야 한다. 또한, 상기 제1 사용자 장치(200)는 A원의 전자 화폐를 상기 제 2사용자 장치(300)에게 전이하기 위해 은행 장치(100)로부터 전자 화폐(c_{u1}, 단, $c_{u1}{}^{eB} \bmod n_B = h(g^r \| ID_{pu1})$)를 인출하며, 제 2사용자 장치(300)는 도 4에 나타난 인출 과정을 수행하여 은행 장치(100)로부터 빈 동전($c_{u2,z}$)을 얻는다. 이 때, $C_{u2,z}{}^{eB,z} \bmod n_{B,z} = h(g^{r^*} \| ID_{u2})$이며, r^*은 난수이고, $d_{B,z}$, $n_{B,z}$ 는 각각 0원의 동전을 나타내는 은행 장치(100)의 비밀키 및 공개 모듈러스이다.

상기와 같은 조건을 만족한 상태에서, 도 8을 참조하여 본 발명의 전이 과정을 설명하면, 먼저, 상기 제 1사용자 장치(200)가 전자 화폐(c_{u1}), 자신의 공개키(P_{u1}) 및 자신의 인증서($Cert_{u1}$), $w(= g^r \bmod p)$를 제 2사용자 장치(300)로 전송(S801)하면, 상기 제 2사용자 장치(300)는 상기 제 1사용자 장치(200)의 인증서($Cert_{u1}$) 및 전자 화폐(c_{u1})의 유효성을 확인(S802)한 후 ($Cert_{u1}{}^{eCA} \bmod n_{CA} = h(ID_{CA} \| ID_{pu1})$, $c_{u1}{}^{eB} \bmod n_B = h(w \| ID_{pu1})$), 챌린저 값($d = h(c_{u1} \| Itime \| c_{u2,z})$)을 계산(S803)하고, 자신의 빈 동전($c_{u2,z}$) (black coin, 액면 금액 0원), 공개키(P_{u2}), 인증서($Cert_{u2}$), 트랜잭션 발생 시각(time), $w^* (= g^{r^*} \bmod p)$등의 정보를 상기 제 1사용자 장치(200)에게 전송(S804)한다.

그러면, 상기 제 1사용자 장치(200)는 제 2사용자 장치(300)의 인증서($Cert_{u2}$) 및 빈 동전($C_{u2,z}$)의 유효성을 확인(S805) ($Cert_{u2}{}^{eCA} \bmod n_{CA} = h(ID_{CA} \| ID_{pu2})$, $C_{u2,z}{}^{eB,z} \bmod n_{B,z} = h(w^* \| ID_{u2})$) 한 후, 상기 제 2사용자 장치(200)와 똑같이 챌린저 값($d = h(c_{u1} \| Itime \| c_{u2,z})$) 및 반응값($z = (r + S_u d) \bmod q$)을 계산(S806)하여, 상기 반응값($z$)을 제 2사용자 장치(300)에게 전송(S807)한다.

제 2사용자 장치(300)는 $w' = g^z p_{u1}{}^d \bmod p$를 계산한 다음 전이된 동전을 확인(S808)한다($c_{u1}{}^{eB} \bmod n_B = h(w' \| ID_{u1})$).

도 9는 본 발명의 전자 현금 거래 방법에 의해 전이된 전자 화폐의 지불 과정에 대한 절차도로서, 상기 제 2사용자 장치(300)가 상기 제 1사용자 장치(200)로 부터 전이된 A원의 전자 화폐($c_{u2,z}$)를 상점 장치(400)로 지불하고자 할 때, 도 9에 나타난 바와 같은 과정을 수행한다. 이 때, $H_{1,2}$는 제 1사용자 장치(200)로부터 제 2사용자 장치(300)로 전이된 A원의 전자 화폐 관련 전이 기록이다.

도 9를 참조하면, 본 발명에서 제공하는 전이된 전자 화폐 지불 과정은 먼저, 상기 제2 사용자 장치(300)가 상기 제1 사용자 장치(200)로부터 전이된 전자 화폐에 관한 전이 기록($H_{1,2} = \{ c_{u2,z}$ z, d, cul, time, w, w^*, $p_{ul} \cdot Cert_{ul}$, $p_{u2} \cdot Cert_{u2}$ }을 상기 상점 장치(400)에게 전송(S901)하면, 상기 상점 장치(400)는 상기 제1 사용자 장치의 인증서($Cert_{ul} {}^{eCA}$ $modn_{CA} = h(ID_{CA}\ IIP_{ul})$)와 상기 제2 사용자 장치의 인증서($Cert_{u2} {}^{eCA}$ $mod_{CA} = h(ID_{CA}\ IIP_{u2})$)를 확인(S902)한 후, 상기 제1 사용자 장치로부터 전이된 동전(C_{ul})의 유효성을 확인(S903)한 후, 상기 모든 확인 과정이 통과되면, 그의 계좌 번호(As)와 트랜잭션 발생 시각(time')을 상기 제2 사용자 장치(300)에게 전송(S904)한다.

상기 제 2사용자 장치(300)는 챌린저 값($d' = h(AsIItime'IIc_{u2,z})$)과 반응값($z = (r^* + S_{u2}\ d') \bmod q$)을 각각 계산(S905)한 후 반응값(z)을 상기 상점 장치(400)에 전송(S906)하고, 상기 상점 장치(400)는 상기 제 2사용자 장치(300)와 동일하게 챌린저 값($d' = h(AsIItime'IIc_{u2,z})$)과, $w'' = g^z p_{u2}{}^{d'} \bmod p$를 계산(S907)하고 전이된 동전($C_{u2}$)의 유효성을 확인($c_{u2,z} {}^{eB,z}$ $modn_{B,z} = h(w''\ IIp_{u2})$)(S908)한다.

이 때, 단계 S904에서 상기 제 2사용자 장치가 제 1사용자 장치로부터 전이된 동전(c_{u1})와 유효성을 확인하기 위해, 전이 기록 $H_{1,2}$에 대한 동전($c_{u2,z}$)의 유효성을 확인하기 위해서는, 먼저, 동전(c_{u1})이 은행 장치(100)의 전자 서명을 포함하고 있는가를 확인($c_{ul} {}^{eB}$ $modn_B = h(wIIp_{u1})$)하고, 동전($c_{u2,z}$)이 은행 장치(100)의 전자 서명을 포함하고 있는가를 확인($c_{u2} {}^{eB,z}$ $modn_{B,z} = h(w^*IIp_{u2})$)하며, 동전($c_{u2,z}$)이 동전($c_{u1}$)으로부터 적법하게 전이되었는지를 확인($d = h(c_{u1}\ IItimeIIc_{u2,z})$, $w' = g^z p_{u1}{}^d \bmod p$. $c_{ul} {}^{eB}$ $modn_B = h(w'IIp_{ul})$)한다.

이 때, 상기와 같이 다른 사용자 장치로부터 동전을 전이 받고자 하는 사용자 장치는 반드시 은행 장치로부터 빈 동전을 얻어야 하며, 상기 빈 동전을 얻지 못하면, 다른 사용자 장치의 동전을 전이 받을 수 없다.

발명의 효과

상기와 같은 본 발명에 따른 전자 현금 거래 방법은 전자 화폐의 인출, 지불, 결제 과정이 간단하며 특히 인출 단계에서 사용자 장치에게 부과되는 계산량이 작고 이 또한 대부분 사전 계산 가능하다는 점에서 효율적이다. 또한, 본 전자 화폐는 위조 불가, 익명성, 이중 사용 탐지, 누명 불가 등 전자 상거래에 필수 불가결한 요구 조건들을 모두 만족시킴으로써 인터넷 상에서 사용자들이 안심하고 쓸 수 있다. 따라서, 본 발명은 효율성이 중시되는 소액권 전자 거래 시스템에서부터 안전성이 더 중시되는 고액권의 전자 거래 시스템에 이르기까지 범용적으로 사용될 수 있다.

또한, 다음과 같은 효과가 있다.

첫째, 은행장치가 이중 사용자를 사후 추적할 수 있다.

즉, 사용자 장치가 서로 다른 챌린저 값 d와 d'에 대하여 동일한 동전을 두번 사용하였다면, 상기 은행 장치는 이 값들로부터 $z = (r + s_u d) \bmod q$ 와 $z' = (r + s_u d') \bmod q$를 계산하고, 수식 $s_u = (z - z')/(d - d') \bmod q$을 계산함으로써 이중 사용자의 비밀키(Su)를 알아낼 수 있으며, 상기 비밀키를 인증기관 장치에게 이중 사용자의 증거로 제시함으로써 이중 사용자를 사후 추적할 수 있다.

둘째, 전자 화폐를 적법하게 사용하는 사용자 장치의 익명성과 프라이버시가 보장된다.

우리의 전자 화폐는 상기 은행 장치에 의하여 서명되는데 상기 은행 장치는 특정 전자 화폐를 특정 사용자 장치에게 연결시킬 수 없다. 왜냐하면 은행 장치는 상기 고객장치의 공개키로부터 고객 장치의 신원 정보를 알아낼 수 없기 때문이다.

셋째, 은행 장치는 인증기관 장치의 도움을 받음으로써 조건부 추적이 가능하다.

앞에서도 언급했듯이, 상기 사용자 장치의 프라이버시를 무조건적으로 보호하게 되면 돈 세탁이나 공갈 등과 같은 범죄 문제들을 야기할 수도 있지만, 본 발명에서는 인증기관 장치가 익명의 공개키와 그 소유자 정보를 갖고 있으므로, 신뢰받는 제 3의 기관 예를 들면, 법원의 허락 아래 인증기관 장치의 도움을 받아 의심스러운 혹은 불법적인 사용자 장치를 추적할 수 있다.

넷째, 은행 장치가 발행하는 전자 화폐는 위조할 수 없다.

본 발명의 전자 화폐를 위조하기 위해서는 $(x, h(x)^{dB} \bmod n_B)$쌍을 위조하여야 한다. 즉, RSA 서명 체계를 깨뜨려야 한다. 그러나, 이것은 nB의 소인수가 알려지지 않으면 거의 불가능한 것으로서, n_B의 소인수는 상기 은행 장치에게만 알려지므로, 은행장치를 제외한 다른 장치가 전자 화폐를 만드는 것은 불가능하다.

다섯째, 은행 장치가 적법한 사용자 장치에게 누명을 씌울 수 없다.

상기 은행 장치가 특정 사용자 장치를 이중 사용자로 누명 씌우기 위해서는 이중 사용의 증거로서 해당 사용자의 비밀키를 제시하여야 하는데, 이산 대수 가정하에서는, 상기 사용자 장치가 프로시저를 따르고 이중 사용하지 않으면, 상기 은행 장치가 상기 사용자 장치의 비밀키를 계산할 수 없다. 즉, 상기 사용자 장치는 누명으로부터 계산적으로 보호된다.

(57) 청구의 범위

청구항 1.

사용자 장치가 은행 장치와 별개인 인증기관 장치로부터 인증서를 발급 받는 인증서 발급 과정;

사용자 장치가 상기 인증서를 사용하여 자신의 신분을 은행 장치에 노출시키지 않고 은행 장치에 자신의 계좌를 개설하는 계좌 개설 과정;

사용자 장치가 상기 개설된 계좌로부터 은행 장치의 서명이 부여된 전자 현금을 인출하는 전자 현금 인출 과정;

상기 사용자 장치가 은행 장치와 오프라인 상태에서 인증서 및 전자 현금을 사용하여 특정 상거래에 대한 지불을 수행하는 전자 현금 지불 과정으로 이루어지되,

상기 인증서 발급 과정은,

사용자 장치가 이산 대수형 서명 체계를 이용하여 사용자의 비밀키 및 공개키를 생성하는 단계;

사용자 장치가 인증기관 장치에게 자신의 신원을 입증하면서 상기 사용자 장치의 공개키를 전송하는 단계;

인증기관 장치가 인증기관 장치의 비밀키, 사용자 장치의 공개키 및 인증기관 장치의 신원 정보를 사용하여 상기 사용자 장치의 공개키에 대한 인증서를 생성하는 단계:

상기 인증기관 장치가 인증서를 사용자 장치에 전송하는 단체 및

사용자 장치가 상기 인증기관 장치의 공개키, 인증기관 장치의 신원 정보 및 사용자 장치의 공개키를 사용하여 상기 인증서의 유효성을 확인하는 단계로 이루어지고,

상기 인증서를 생성하는 단계에서,

상기 인증서의 생성은 아래의 수학식을 이용하는 전자 현금 거래 방법.

$$Cert_u = h(ID_{CA} \| p_u)^{d_{CA}} \bmod n_{CA}$$

여기서, 상기 $Cert_u$는 인증서, ID_{CA} 는 인증기관 장치의 신원 정보, p_u는 사용자 장치의 공개키, d_{CA} 는 인증기관 장치의 비밀키, n_{CA} 는 인증기관 장치의 공개 모듈러스, h는 일방향 함수이다.

청구항 2.

제 1항에 있어서 ,

상기 공개키를 생성하는 단계에서 공개키의 생성은 아래의 수학식을 이용하는 전자 현금 거래 방법.

$$p_u = g^{-S_U} \bmod p$$

여기서, P_U는 사용자 장치의 공개키, S_U는 사용자 장치의 비밀키, g는 Z^*_p의 부분군 G_q의 생성자이다.

청구항 3.

제1항에 있어서,

상기 인증서의 유효성을 확인하는 단계에서, 유효성의 확인은 아래의 수학식을 이용하는 전자 현금 거래 방법.

$$Cert_u^{e_{CA}} \bmod n_{CA} = h(ID_{CA} \| p_u)$$

여기서, 상기 $Cert_u$는 인증서, ID_{CA} 는 인증기관 장치의 신원 정보, p_u는 사용자 장치의 공개키, eCA는는 인증기관 장치의 비밀키, n_{CA} 는 인증기관 장치의 공개 모듈러스, h는 일방향 함수이다.

청구항 4.

제1항에 있어서,

상기 계좌 개설 과정은,

사용자 장치가 사용자 장의 공개키 및 그에 상응하는 인증서를 은행 장치로 전송하는 단계;

은행 장치가 상기 사용자 장치의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계 및

상기 사용자 장치의 공개키 및 그에 상응하는 인증서가 유효하면 상기 은행 장치가 상기 사용자 장치의 공개키에 대한 계좌를 개설하는 단계를 포함하는 전자 현금 기래 방법.

청구항 5.

사용자 장치가 은행 장치와 별개인 인증기관 장치로부터 인증서를 발급 받는 인증서 발급 과정;

사용자 장치가 상기 인증서를 사용하여 자신의 신분을 은행 장치에 노출시키지 않고 은행 장치에 자신의 계좌를 개설하는 계좌 개설 과정;

사용자 장치가 상기 개설된 계좌로부터 은행 장치의 서명이 부여된 전자 현금을 인출하는 전자 현금 인출 과정;

상기 사용자 장치가 은행 장치와 오프라인 상태에서 인증서 및 전자 현금을 사용하여 특정 상거래에 대한 지불을 수행하는 전자 현금 지불 과정으로 이루어지되,

상기 인증서 발급 과정은,

사용자 장치가 이산 대수형 서명 체계를 이용하여 사용자의 비밀 키 및 공개키를 생성하는 단계;

사용자 장치가 인증기관 장치에게 자신의 신원을 입증하면서 상기 사용자 장치의 공개키를 전송하는 단계;

인증기관 장치가 인증기관 장치의 비밀키, 사용자 장치의 공개키 및 인증기관 장치의 신원 정보를 사용하여 상기 사용자 장치의 공개키에 대한 인증서를 생성하는 단계;

상기 인증기관 장치가 상기 인증서를 사용자 장치에 전송하는 단계 및 사용자 장치가 상기 인증기관 장치의 공개키, 인증기관 장치의 신원 정도 및 사용자 장치의 공개키를 사용하여 상기 인증서의 유효성을 확인하는 단계로 이루어지고,

상기 사용자 장치 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계에서 공개키 및 인증서의 확인은 아래의 수학식을 이용하는 전자 현금 거래 방법.

$$Cert_u^{e_{CA}} \bmod n_{CA} = h(ID_{CA} \| p_u)$$

여기서, 상기 Certu는 인증서, IDCA는 인증기관 장치의 신원 정보, pu는 사용자 장치의 공개키, eCA는 인증기관 장치의 공개키, nCA는 인증기관 장치의 공개 모듈러스, h는 일방향 함수이다.

청구항 6.

제5항에 있어서,

상기 전자 현금 인출 과정은,

상기 사용자 장치가 전자 현금 난수를 발생하고 상기 전자 현금 난수에 대한 이미지를 생성하는 단계;

상기 사용자 장치가 전자 현금 인출을 위한 메시지를 생성하고 상기 메시지글 은닉하는 단계;

상기 사용자 장치가 상기 메시지에 관한 사용자 장치의 서명을 생성하는 단계;

상기 사용자 장치가 상기 메시지, 상기 사용자 장치의 서명, 사용자 장치의 공개키 및 그에 상응하는 인증서를 전송하는 단계;

상기 은행 장치에서 사용자 장치의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계;

상기 은행 장치가 상기 사용자 장치 서명의 유효성을 확인하는 단계;

상기 사용자 장치의 공개키 및 그에 상응하는 인증서 그리고 상기 서명이 모두 유효하면 상기 은행 장치가 상기 은닉된 메시지에 은행 장치의 서명을 하는 단계;

상기 은행 장치가 상기 은행 장치에 서명된 메시지를 상기 사용자 장치로 전송하는 단계;

상기 사용자 장치가 상기 은행 장치로부터 은행 장치에 서명된 메시지를 얻고, 얻은 메시지와 상기 발생된 난수를 전자 현금으로 저장하는 단계를 포함하는 전자 현금 거래 방법.

청구항 7.

제6항에 있어서,

상기 은행 장치에서 상기 인출된 전자 현금에 상응하는 금액을 상기 사용자 장치의 개좌에서 감소시키는 전자 현금 거래 방법.

청구항 8.

사용자 장치가 은행 장치와 별개인 인증기관 장치로부터 인증서를 발급 받는 인증서 발급 과정;

사용자 장치가 상기 인증서를 사용하여 자신의 신분을 은행 장치에 노출시키지 않고 은행 장치에 자신의 계좌를 개설하는 계좌 개설 과정;

사용자 장치가 상기 개설된 계좌로부터 은행 장치의 서명이 부여된 전자 현금을 인출하는 전자 현금 인출 과정;

상기 사용자 장치가 은행 장치와 오프라인 상태에서 인증서 및 전자 현금을 사용하여 특정 상거래에 대한 지불을 수행하는 전자 현금 지불 과정으로 이루어지되,

상기 전자 현금 인출 과정은,

상기 사용자 장치가 전지 현금 난수를 발생하고 상기 전자 현금 난수에 대한 이미지를 생성하는 단계;

상기 사용자 장치가 전자 현금 인출을 위한 메시지를 생성하고 상기 메시지를 은닉하는 단계;

상기 사용자 장치가 상기 메시지에 관한 사용자 장치의 서명을 생성하는 단계;

상기 사용자 장치가 상기 메시지, 상기 사용자 장치의 서명, 사용자 장치의 공개키 및 그에 상응하는 인증서를 전송하는 단계;

상기 은행 장치에서 사용자 장치의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계;

상기 은행 장치가 상기 사용자 장치 서명의 유효성을 확인하는 단계;

상기 사용자 장치의 공개키 및 그에 상응하는 인증서 그리고 상기 서명이 모두 유효하면 상기 은행 장치가 상기 은닉된 메시지에 은행 장치의 서명을 하는 단계;

상기 은행 장치가 상기 은행 장치에 서명된 메시지를 상기 사용자 장치로 전송하는 단계;

상기 사용자 장치가 상기 은행 장치로부터 은행 장치에 서명된 메시지를 얻고, 얻은 메시지와 상기 발생된 난수를 전자 현금으로 저장하는 단계로 이루어지고,

상기 사용자 장치 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계에서 공개키 및 인증서의 확인은 아래의 수학식을 이용하는 전자 현금 거래 방법.

$$Cert_u^{e_{CA}} \bmod n_{CA} = h(ID_U \| p_u)$$

여기서, 상기 Certu는 인증서, IDCA는 인증기관 장치의 신원 정보, pu는 사용자 장치의 공개키, eCA는 인증기관 장치의 공개키, nCA는 인증기관 장치의 공개 모듈러스, h는 일방향 함수이다.

청구항 9.

제8항에 있어서,

상기 전자 현금 난수에 대한 이미지를 생성하는 단계에서의 난수는,

{1, ..., q}에서 랜덤하게 선택된 어느 하나이고, 상기 난수의 이미지는 아래의 수학식에 따라 생성되는 전자 현금 거래 방법.

$$r' = g^{r} \bmod p$$

여기서, r은 난수, r'는 이미지, g는 Z^{*}_{p}의 G(q)의 생성자이고, q는 G(q)의 위수이다.

청구항 10.

제8항에 있어서,

상기 전자 현금 인출을 위한 메시지를 생성하는 단계에서, 메시지 생성은 아래의 수학식을 이용하는 전자 현금 거래 방법.

$$h(r' \| P_U)$$

여기서, P_U는 사용자 장치의 공개키, r'는 난수의 이미지, h는 일방향 함수이다.

청구항 11.

제8항에 있어서,

상기 은행 장치가 상기 은닉된 메시지에 은행 장치의 서명을 하는 단계는 아래의 수학식을 이용하여 은행 장치에 서명된 메시지를 생성하는 전자 현금 거래 방법.

$$c = [c']^{dB} \bmod nB$$

여기서, dB는 은행 장치의 비밀키, nB는 은행 장치의 공개 모듈러스, c는 은행장치에 서명된 메시지, c'는 은닉된 메시지이다.

청구항 12.

제8항에 있어서 ,

상기 사용자 장치를 지불자라고 하고, 그의 상거래 상대방을 피지불자라고 할 때, 상기 전자 현금 지불 과정은,

상기 지불자가 전자 현금 메시지, 그 자신의 공개키 및 그에 상응하는 인증서를 피지불자에게 전송하는 단계;

피지불자는 상기 지불자의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계;

상기 피지불자의 은행 계좌 번호 및 거래 시간을 상기 지불자에게 전송하는 단계;

상기 피지불자가 상기 전자 현금 메시지, 그에 은행 계좌 번호 및 상기 거래 시간에 근거하여 챌린저값을 산출하는 단계;

상기 지불자가 상기 전자 현금에 관련된 난수, 상기 챌린저값, 지불자의 비밀키를 이용하여 상기 챌린저값에 대한 반응값을 생성하는 단계;

상기 지불자가 상기 반응값을 상기 지불자에게 전송하는 단계;

상기 피지불자가 상기 반응값의 유효성을 확인하는 단계;

상기 반응값이 유효하면, 상기 피지불자가 상기 전자 현금을 받아들이는 단계를 포함하는 전자 현금 거래 방법.

청구항 13.

사용자 장치가 은행 장치와 별개인 인증기관 장치로부터 인증서를 발급 받는 인증서 발급 과정;

사용자 장치가 상기 인증서를 사용하여 자신의 신분을 은행 장치에 노출시키지 않고 은행 장치에 자신의 계좌를 개설하는 계좌 개설 과정;

사용자 장치가 상기 개설된 계좌로부터 은행 장치의 서명이 부여된 전자 현금을 인출하는 전자 현금 인출 과정;

상기 사용자 장치가 은행 장치와 오프라인 상태에서 인증서 및 전자 현금을 사용하여 특정 상거래에 대한 지불을 수행하는 전자 현금 지불 과정으로 이루어지되,

상기 사용자 장치를 지불자라고 하고, 그의 상거래 상대방을 피지불자라고 할 때, 상기 전자 현금 지불 과정은,

상기 지불자가 전자 현금 메시지, 그 자신의 공개키 및 그에 상응하는 인증서를 피지불자에게 전송하는 단계;

피지불자는 상기 지불자의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계;

상기 피지불자의 은행 계좌 번호 및 거래 시간을 상기 지불자에게 전송하는 단계;

상기 피지불자가 상기 전자 현금 메시지, 그에 은행 계좌 번호 및 상기 거래 시간에 근거하는 챌린저값을 산출하는 단계;

상기 지불자가 상기 전자 현금 메시지, 상기 피지불자의 은행 계좌 번호 및 상기 거래 시간에 근거하는 챌린저값을 산출하는 단계;

상기 지불자가 상기 전자 현금 메시지, 상기 피지불자의 은행 계좌 번호 및 상기 거래 시간에 근거하여 챌린저값 산출하는 단계;

상기 지불자가 상기 전자 현금에 관련된 난수, 상기 챌린저값, 지불자의 비밀키를 이용하여 상기 챌린저값에 대한 반응값을 생성하는 단계;

상기 지불자가 상기 반응값을 상기 지불자에게 전송하는 단계;

상기 피지불자가 상기 반응값의 유효성을 확인하는 단계;

상기 반응값이 유효하면, 상기 피지불자가 상기 전자 현금을 받아들이는 단계를 포함하고:

여기기서, 상기 피지불자가 지불자의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계에서의 유효성 확인은 아래의 수학식을 이용하는 전자 현금 거래 방법.

$$Cert_u^{e_{CA}} \bmod n_{CA} = h(ID_{CA} \| p_u)$$

여기서, 상기 $Cert_u$는 인증서, ID_{CA} 는 인증기관 장치의 신원 정보, p_u는 사용자 장치의 공개키, e_{CA} 는 인증기관 장치의 공개키, n_{CA} 는 인증기관 장치의 공개 모듈러스, h는 일방향 함수이다.

청구항 14.

제13항에 있어서,

상기 피지불자가 상기 전자 현금 메시지 c, 그에 은행 계좌 번호 As 및 상기 거래 시간 time에 근거하여 챌린저값 d를 산출하는 단계에서 상기 챌린값은 아래의 수학식을 이용하여 산출하는 전자 현금 거래 방법.

$$d = h(A_s \| time \| c)$$

여기서, h는 일방향 함수이다.

청구항 15.

제13항에 있어서 ,

상기 피지불자가 상기 전자 현금 메시지 c, 상기 피지불자의 은행 계좌 번호 As 및 상기 거래 시간 time에 근거하여 챌린저값 d를 산출하는 단계에서 상기 챌린값은 아래의 수학식을 이용하여 산출하는 전자 현금 거래 방법.

$$d = h(A_s \| time \| c)$$

여기서, h는 일방향 함수이다.

청구항 16.

제13항에 있어서,

상기 지불자가 상기 전자 현금에 관련된 난수, 상기 챌린저 값, 지불자의 비밀키를 사용하여 상기 챌린저값에 대한 반응값을 생성하는 단계에서, 챌린저값에 대한 반응값의 생성은 아래의 수학식을 이용하는 현금 거래 방법.

$$z = (r + Sd) \bmod q$$

여기서, r은 전자 현금에 관련된 난수, d는 상기 챌린저 값 , S_U는 지불자의 비밀키, z는 챌린저값에 대한 반응값이다.

청구항 17.

제13항에 있어서,

상기 피지불자가 상기 반응값의 유효성을 확인하는 단계는, 아래의 수학식이 성립하는지를 확인함으로써 이루어지는 전자 현금 거래 방법.

$$c^{eB} \bmod n_B = h(g^z P_U \bmod P \| P_U)$$

여기서, eB는 은행 장치의 공개키, nB는 은행 장치의 공개 모듈러스, Pu는 지불자의 공개키, d는 챌린저 값, z는 반응값, g는 Z*p의 부분군 G(q)의 생성자, h는 일방향 함수임.

청구항 18.

제15항에 있어서,

상기 피지불자는 상점 장치인 전자 현금 거래 방법.

청구항 19.

제15항에 있어서,

상기 전자 현금을 지불 받는 피지불자가 상기 전자 현금에 관련된 기록들을 상기 은행 장치에 제출하여 피지불자 계좌의 상기 전자 현금을 예치하는 전자 현금 결제 과정을 더 포함하는 전자 현금 거래 방법.

청구항 20.

제19항에 있어서,

상기 전자 현금 결제 과정은,

상기 사용자 장치를 지불자라고 할 때, 상기 피지불자가 은행 장치로 전자 현금 메시지, 지불자의 공개 키 및 그에 상응하는 인증서, 챌린저값, 거래 시간, 피 지불자의 계좌번호 및 반응값을 전송하는 단계;

은행 장치가 지불자의 공개키 및 그에 상응하는 인증서의 유효성 및 상기 반응값의 유효성을 확인하는 단계;

은행 장치가 상기 전자 현금이 그 자신의 예치 데이터베이스에 저장되어 있는지를 확인하는 단계를 포함하는 전자 현금 거래 방법.

청구항 21.

재20항에 있어서,

상기 은행 장치가 지불키의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계에서 공개키 및 인증서의 유효성 확인은 아래의 수학식을 이용하는 전자 현금 거래 방법.

$$Cert_u^{e_{CA}} \bmod n_{CA} = h(ID_{CA} \| p_u)$$

여기서, 상기 Certu는 인증서, IDCA는 인증기관 장치의 신원 정보, pu는 사용자 장치의 공개키, eCA는 인증기관 장치의 공개키, nCA는 인증기관 장치의 공개 모듈러스, h는 일방향 함수이다.

청구항 22.

제20항에 있어서,

상기 은행 장치가 상기 반응값의 유효성을 확인하는 단계에서 유효성 확인은 아래의 수학식을 이용하는 전자 현금 거래 방법.

$$c^{e_B} \bmod n_B = h(g^d P_U \bmod P \| P_U)$$

여기서, eB는 은행 장치의 공개키, nB는 은행 장치의 공개 모듈러스, Pu는 지불자의 공개키, d는 챌린저 값, z는 반응값, g는 Z*p의 부분군 G(q)의 생성자, h는 일방향 함수임.

청구항 23.

제13항에 있어서,

상기 전자 현금 지불 과정은 지불자인 상기 사용자 장치가 소유하고 있는 전자 현금을 복수로 분할하여 그 일부만을 지불하는 전자 현금 거래 방법.

청구항 24.

사용자 장치가 은행 장치와 별개인 인증기관 장치로부터 인증서를 발급 받는 인증서 발급 과정;

사용자 장치가 상기 인증서를 사용하여 자신의 신분을 은행 장치에 노출시키지 않고 은행 장치에 자신의 계좌를 개설하는 계좌 개설 과정;

사용자 장치가 상기 개설된 계좌로부터 은행 장치의 서명이 부여된 전자 현금을 인출하는 전자 현금 인출 과정;

상기 사용자 장치가 은행 장치와 오프라인 상태에서 인증서 및 전자 현금을 사용하여 특정 상거래에 대한 지불을 수행하는 전자 현금 지불 과정으로 이루어지되,

상기 전자 현금 지불 과정은,

지불자가 지급 현금 난수 r_1 및 잔여 전자 현금 난수 r_2를 선택하는 단계;

상기 지불자가 상기 지급 전자 현금 난수 및 잔여 현금 난수의 이미지들 r'_1 r'_2를 생성하는 단계;

상기 지불자가 상기 전자 현금 메시지 c, 상기 전자 현금 난수의 이미지 r', 상기 전자 현금의 금액 A, 지급 전자 현금 난수의 이미지 r'_1, 지급 전자 현금의 금액 A_1 및 잔여 전자 현금 난수의 이미지 r'_2에 근거하여 전자 현금 메시지 서명 d를 산출하고, 이에 상응하는 전자 현금 메시지 서명 반응값 z를 상기 전자 현금 메시지 서명 d, 지불자의 비밀키 S_U상기 전자 현금 난수 r을 사용하여 생성하는 단계;

상기 지불자가 피지불자에게 전자 현금 메시지 c, 상기 전자 현금 난수의 이미지 r', 상기 전자 현금의 금액 A, 지급 전자 현금 난수의 이미지 r'_1, 지급 전자 현금의 금액 A_1, 잔여 전자 현금 난수의 이미지 r'_2, 상기 전자 현금 메시지 서명 d, 지불자의 공개키 P_U 및 그에 상응하는 인증서 $Cert_U$를 피지불자에게 전송하는 단계;

피지불자는 상기 지불자의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계;

상기 피지불자의 은행 계좌 번호 및 거래 시간을 상기 지불자에게 전송하는 단계;

상기 피지불자가 지급 전자 현금 난수의 이미지 r'_1, 지급 전자 현금의 금액 A_1, 그의 은행 계좌번호 As 및 거래 시간 time에 근거하여 챌린저값 d_1을 산출하는 단계;

상기 지불자가 상기 지급 전자 현금 난수의 이미지 r'_1, 지급 전자 현금의 금액 A_1, 상기 피지불자의 은행 계좌번호 As 및 상기 거래 시간 time, 지불자의 비밀키 S_U, 전자 현금 난수 r에 근거하여 상기 챌린저값에 대한 반응값 z_1을 생성하는 단계;

상기 지불자가 상기 반응값을 상기 피지불자에게 전송하는 단계;

상기 피지불자가 상기 챌린저값에 대한 반응값 z_1의 유효성을 확인하는 단계;

상기 반응값이 유효하면 상기 피지불자가 상기 전자 현금을 받아들이는 단계를 포함하는 전자 현금 거래 방법.

청구항 25.

제24항에 있어서,

상기 지불자가 상기 지급 전자 현금 난수 및 잔여 현금 난수의 이미지들 r'_1, r'_2를 생성하는 단계는 아래의 수학식에 의해 생성되는 전자 현금 거래 방법.

$$r_1' = g^{r_1} \bmod p$$

$$r_2' = g^{r_2} \bmod p$$

청구항 26.

제24항에 있어서,

상기 지불자가 상기 전자 현금 메시지 c, 상기 전자 현금 난수의 이미지 r', 상기 전자 현금의 금액 A, 지급 전자 현금 난수의 이미지 r'_1, 지급 전자 현금의 금액 A_1 및 잔여 전자 현금 난수의 이미지 r'_2에 근거하여 전자 현금 메시지 서명 d를 산출하고, 이에 상응하는 전자 현금 메시지 서명 반응값 z를 상기 전자 현금 메시지 서명 d, 지불자의 비밀키 S_U 및 상기 전자 현금 난수 r을 사용하여 생성하는 단계는 아래의 수학식에 따라 이루어지는 전자 현금 거래 방법.

$$d = h(c \| r' \| A \| r_1' \| A_1 \| r_2')$$

$$z = (r + s_U d) \bmod q$$

여기서, h는 일방향 함수임.

청구항 27.

제24항에 있어서,

상기 피지불자는 상기 지불자의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계에서 유효성의 확인은 아래의 수학식에 따라 이루어지는 전자 현금 거래 방법.

$$Cert_u^{eCA} \bmod n_{CA} = h(ID_{CA} \| p_u)$$

여기서, 상기 Certu는 인증서, IDCA는 인증기관 장치의 신원 정보, pu는 사용자 장치의 공개키, eCA는 인증기관 장치의 공개키, nCA는 인증기관 장치의 공개 모듈러스, h는 일방향 함수이다.

청구항 28.

제24항에 있어서,

상기 피지불자가 지급 전자 현금 난수의 이미지 r'_1, 지급 전자 현금의 금액 A_1, 그의 은행 계좌번호 As 및 거래 시간 time에 근거하여 챌린저값 d1을 산출하는 단계에서 챌린저 값은 아래의 수학식을 이용하여 산출하는 전자 현금 거래 방법.

$$d_1 = h(r_1' \| A_1 \| A_S \| time)$$

여기서, h는 일방향 함수임.

청구항 29.

제24항에 있어서,

상기 지불자가 상기 지급 전자 현금 난수의 이미지 r'_1, 지급 전자 현금의 금액 A_1, 상기 피지불자의 은행 계좌번호 As 및 상기 거래 시간 time, 지불자의 비밀키 S_U, 전자 현금 난수 r에 근거하여 상기 챌린저값에 대한 반응값 z_1을 생성하는 단계는,

상기 지불자가 아래의 수학식을 이용하여 챌린저 값 d_1을 산출하는 단계;

$$d_1 = h(r_1' \| A_1 \| A_S \| time)$$

여기서, h는 일방향 함수임.

상기 지불자가 아래의 수학식을 이용하여 상기 챌린저값에 상응하는 반응값 z_1을 산출하는 단계를 포함하는 전자 현금 거래 방법.

$$z_1 = (r + s_U d_1) \bmod q$$

청구항 30.

제24항에 있어서,

상기 피지불자가 상기 챌린저값에 대한 반응값 z_1 의 유효성을 확인하는 단계는 아래의 수학식이 성립함을 확인함으로써 수행되는 전자 현금 거래 방법.

$$c^{eB} \bmod n_B = h(g^{z1} P_U^{d1} \bmod P \| P_W)$$

여기서, eB는 은행 장치의 공개키, nB는 은행 장치의 공개 모듈러스, Pu는 지불자의 공개키, d1는 챌린저 값, z1는 반응값, g는 Z*p의 부분군 G(q)의 생성자, h는 일방향 함수임.

청구항 31.

제24항에 있어서,

상기 지불자는 아래의 수학식을 이용하여 중간값 w_1 을 산출하는 단계를 더 포함하는 전자 현금 거래 방법.

$$w_1 = g^{r1} \, p_W^{d1} \bmod p$$

청구항 32.

제31항에 있어서,

상기 지불자는 전자 현금 메시지 c, 전자 현금 난수 이미지 r', 전자 현금 금액 A, 지급 전자 현금 난수 이미지 r_1', 지급 전자 현금 금액 A_1, 잔여 전자 현금 난수 이미지 r_2', 챌린저 값 d_1, 중간값 w_1 을 저장하는 단계를 더 포함하는 전자 현금 거래 방법.

청구항 33.

제24항에 있어서,

상기 사용자 장치는 적어도 2 이상이 있으며, 각 사용자 장치에 대해서 상기 인증서 발급 단계 및 상기 계좌 개설 단계를 수행하며, 그중 하나의 사용자 장치를 양도인이라 하고 다른 하나의 사용자 장치를 양수인이라고 할 때, 양도인이 가진 전자 현금을 양수인에게 전이하는 전자 현금 전이 과정을 더 포함하는 전자 현금 거래 방법.

청구항 34.

제33항에 있어서,

상기 전자 현금 전이 과정은,

양수인이 은행 장치로부터 전자 현금 cu2.z을 인출하는 단계;

양도인이 양수인에게 전자 현금 메시지 cU1, 양도인의 공개키 pU1 및 그에 상응하는 인증서 CertU1, 전자 현금 난수 이미지 w를 양수인에게 전송하는 단계;

양수인이 양도인의 공개키 pu1 및 그에 상응하는 인증서 CertU1의 유효성을 확인하는 단계;

양수인이 수신한 전자 현금 cu1의 유효성을 확인하는 단계;

상기 양도인의 공개키 및 그에 상응하는 인증서와 수신한 전자 현금이 유효한 경우, 양수인이 챌린저 값 d를 산출하는 단계;

양수인이 양수인의 빈 전자 현금 메시지 cu2.z, 양수인의 공개키 PU2 및 그에 상응하는 인증서 CertU2, 거래 시간 time, 빈 전자 현금 난수 이미지 w*를 양도인에게 전송하는 단계;

양도인이 양수인의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계;

양도인이 양수인의 빈 전자 현금의 유효성을 확인하는 단계;

양도인이 전자 현금 메시지 CU1, 거래 시간 time, 빈 전자 현금 메시지 CU2.z에 근거하여 챌린저 값 d를 산출하는 단계;

양도인이 상기 챌린저 값d, 양도인의 비밀키 sU1. 전자 현금 난수 r을 사용하여 상기 챌린저 값에 대한 반응값 z를 산출하는 단계;

양도인이 상기 반응값을 양수인에게 전송하는 단계;

양수인이 상기 반응값의 유효성을 확인하는 단계; 를 포함하는 전자 현금 거래 방법.

청구항 35.

제34항에 있어서,

상기 양수인이 은행 장치로부터 빈 전자 현금을 인출하는 단계는,

빈 전자 현금에 대한 난수를 발생하는 단계;

상기 빈 전자 현금 난수에 대한 이미지를 생성하는 단계;

빈 전자 현금 인출을 위한 메시지를 생성하는 단계;

상기 메시지에 관한 양수인의 서명을 생성하는 단계;

상기 메시지, 상기 양수인의 서명, 양수인의 공개키 및 그에 상응하는 인증서를 전송하는 단계;

상기 은행 장치에서 양수인의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계;

상기 양수인 서명에 대한 유효성을 확인하는 단계;

상기 양수인의 공개키 및 그에 상응하는 인증서 그리고 상기 서명이 모두 유효하면, 은행 장치가 상기 은닉된 메시지에 은행 장치의 서명을 하는 단계;

상기 은행 장치가 상기 은행 장치 서명된 메시지를 상기 양수인에게 전송하는 단계;

상기 양수인이 상기 은행 장치로부터 은행 장치 서명된 빈 전자 현금 메시지를 얻는 단계;

상기 양수인이 상기 은행 장치 서명된 빈 전자 현금 메시지와 상기 빈 전자 현금 난수를 빈 전자 현금으로 저장하는 단계;를 포함하는 전자 현금 거래 방법.

청구항 36.

제34항에 있어서,

상기 양수인이 양도인의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계는 아래의 수학식이 성립함을 확인하는 전자 현금 거래 방법.

$$Cert_u^{eCA} \bmod n_{CA} = h(ID_{CA} \| p_u)$$

여기서, 상기 Certu는 인증서, IDCA는 인증기관 장치의 신원 정보, pu는 사용자 장치의 공개키, eCA는 인증기관 장치의 공개키, nCA는 인증기관 장치의 공개 모듈러스, h는 일방향 함수이다.

청구항 37.

제34항에 있어서,

상기 양수인이 수신한 전자 현금 메시지 cU1의 유효성을 확인하는 단계는 아래의 수학식이 성립하는지를 확인하는 전자 현금 거래 방법.

$$c_{U1}^{eB} \bmod n_B = h(w \| P_{U1})$$

여기서, eB는 은행 장치의 공개키, nB는 은행 장치의 공개 모듈러스, PU1는 양도인의 공개키, w는 전자 현금 난수 이미지, h는 일방향 함수임.

청구항 38.

제34항에 있어서,

상기 양수인이 꿸린저 값 d를 산출하는 단계는 아래의 수학식에 따라 이루어지는 전자 현금 거래 방법.

$$d = h(c_{U1} \| w \| P_{U1})$$

여기서, eB는 은행 장치의 공개키, nB는 은행 장치의 공개 모듈러스, PU1는 양도인의 공개키, w는 전자 현금 난수 이미지, h는 일방향 함수임.

청구항 39.

제33항에 있어서,

상기 양수인이 지불자로서 피지불자에게 상기 전자 현금을 상거래에 대한 댓가로서 지불하는 전이된 전자 현금 지불 과정을 더 포함하는 전자 현금 거래 방법.

청구항 40.

제39항에 있어서,

상기 전이된 전자 현금 지불 과정은,

지불자가 피지불자에게 전자 현금 전이 기록 H1,2를 전송하는 단계;

피지불자가 상기 양도인의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계;

피지불자가 상기 지불자의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계;

피지불자가 상기 전이된 전자 현금의 유효성을 확인하는 단계;

피지불자가 지불자에게 피지불자의 계좌번호 및 당해 지불에 관련된 거래 시간을 전송하는 단계;

지불자가 상기 피지불자의 은행 계좌 번호, 거래 시간 및 빈 전자 현금 메시지를 사용하여 챌린저 값 및 그에 상응하는 반응값을 산출하는 단계;

지불자가 상기 반응값을 피지불자에게 전송하는 단계;

피지불자가 상기 반응값의 유효성을 확인하는 단계를 포함하는 전자 현금 거래 방법.

청구항 41.

제40항에 있어서,

상기 전자 현금 전이 기록 H1,2는 빈 전자 현금 메시지 cU2,z, 상기 반응값 z, 챌린저값 d, 전자 현금 메시지 cU1, 전자 현금 양도 시간 time, 전자 현금 난수 이미지 w, 빈 전자 현금 난수 이미지 w*, 양도인의 공개키 pU1 및 그에 상응하는 인증서 CertU1, 지불자의 공개키 PU2 및 그에 상응하는 인증서 CertU2를 포함하는 전자 현금 거래 방법.

청구항 42.

제40항에 있어서,

상기 피지불자가 상기 양도인의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계는 아래의 수학식이 성립하는지를 확인하는 전자 현금 거래 방법.

$$[Certu_1]^{eCA} \bmod n_{CA} = h(IDc_1 \| pu_1)$$

여기서, 상기 Certu1은 양도인의 공개키에 상응하는 인증서, IDCA는 인증기관 장치의 신원 정보, pu1은 양도인의 공개키, eCA는 인증기관 장치의 공개키, nCA는 인증기관 장치의 공개 모듈러스, h는 일방향 함수이다.

청구항 43.

제40항에 있어서,

상기 피지불자가 상기 지불자의 공개키 및 그에 상응하는 인증서의 유효성을 확인하는 단계는 아래의 수학식이 성립되는지를 확인하는 전자 현금 거래 방법.

$$[Certu2]^{eCA} \bmod n_{CA} = h(IDCA \| pu2)$$

여기서, 상기 Certu2는 지불자의 공개키에 상응하는 인증서, IDCA는 인증기관 장치의 신원 정보, pu2는 지불자의 공개키, eCA는 인증기관 장치의 공개키, nCA는 인증기관 장치의 공개 모듈러스, h는 일방향 함수이다.

청구항 44.

제40항에 있어서,

상기 피지불자가 상기 전이된 전자 현금의 유효성을 확인하는 단계는,

전자 현금 메시지가 유효한지를 확인하는 단계;

지불자의 빈 전자 현금 메시지가 유효한지를 확인하는 단계;

전자 현금 전이 과정이 적법하게 이루어졌는지를 확인하는 단계를 포함하는 전자 현금 거래 방법.

청구항 45.

제44항에 있어서,

상기 전자 현금 메시지가 유효한지를 판단하는 단계는 아래의 수학식이 성립하는지를 확인하는 전자 현금 거래 방법.

$$cu1^{eB} \bmod n_B = h(w \| PU_1)$$

여기서, cU1은 전자 현금 메시지, eB는 은행 장치의 공개키, nB는 은행장치의 공개 모듈러스, PU1는 양의 공개키, w는 전자 현금 난수 이미지, h는 일방향 함수임.

청구항 46.

제44항에 있어서,

상기 지불자의 빈 전자 현금 메시지가 유효한지를 확인하는 단계는 아래의 수학식이 성립하는지를 확인함으로써 현금 메시지 내에 은행 장치의 서명이 포함되어 있는지를 확인하는 전자 현금 거래 방법.

$$cu2,z^{eB,z} = \bmod n_{B,z} = h(w' \| pu_2)$$

여기서, cU2,z는 빈 전자 현금 메시지, eB.z는 은행 장치의 공개키, nB.z는 은행 장치의 공개 모듈러스, w8는 빈 전자 현금 난수 이미지, pU2는 지불자의 공개키, h는 일방향 함수임.

청구항 47.

제44항에 있어서,

상기 전자 현금 전이 과정이 적법하게 이루어졌는지를 확인하는 단계는 아래의 수학식이 성립하는지를 확인함으로써 이루어지는 전자 현금 거래 방법.

$$c_{U1}{}^{eB} \bmod n_B = h(g^{Z} p_{U2}{}^{c'} \bmod p \parallel p_{U1})$$

여기서, cU1은 전자 현금 메시지, eB는 은행 장치의 공개키, nB는 은행 장치의 공개 모듈러스, PU1은 양도인의 공개키, d는 챌린저값, g는 Zp*의 부분군 G(q)의 생성자, h는 일방향 함수임.

청구항 48.

제44항에 있어서,

상기 지불자가 상기 피지불자의 은행 계좌 번호, 거래 시간 및 빈 전자 현금 메시지를 사용하여 챌린저값 및 그에 상응하는 반응값을 산출하는 단계는 아래의 수학식을 이용하여 산출하는 전자 현금 거래 방법.

$$d' = h(A_S \parallel time' \parallel c_{U2}.z)$$

$$z = (r + s_{U2}d') \bmod q$$

여기서, d'는 챌린저값, As는 피지불자의 은행 계좌 번호, time'는 거래 시간, cU2.z은 빈 전자 현금 메시지, SU2는 지불자의 비밀키, h는 일방향 함수임.

청구항 49.

제44항에 있어서,

상기 피지불자가 상기 반응값의 유효성을 확인하는 단계는,

피지불자의 은행 계좌 번호 As, 거래시간 time, 빈 전자 현금 메시지 cu2.z를 사용하여 아래의 수학식에 따라 챌린저값 d'를 산출하는 단계;

$$d' = h(A_S \parallel time' \parallel c_{U2}.z)$$

상기 챌린저값 d'와 지불자의 공개키 Pu2, 수신한 반응값 z를 사용하여 아래의 수학식에 따라 중간값 w'를 산출하는 단계;

$$w' = g^{Z} p_{U2}{}^{d'} \bmod p$$

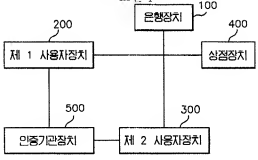
아래의 수학식이 성립하는지를 확인하는 단계를 포함하는 전자 현금 거래 방법.

$$CU2,z^{eB} = mod\ n_B = h(w^{x'} \| p_{UZ})$$

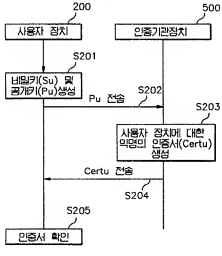
이기서, CU2,z는 빈 전자 현금 메시지, eB는 은행 장치의 공개키, h는 일방향 함수임.

도면

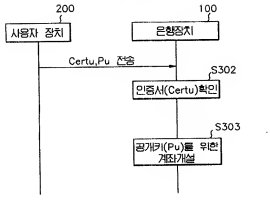
도면 1



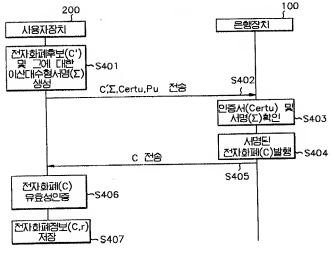
도면 2



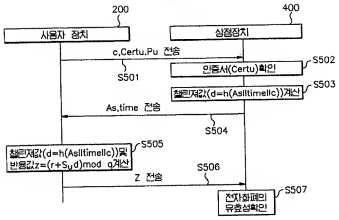
도면 3


200
100
사용자 장치
은행장치
Certu,Pu 전송
S302
인증서(Certu)확인
S303
공개키(Pu)를 위한
계좌개설

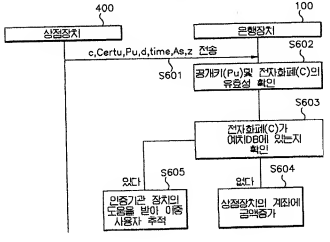
도면 4


200
100
사용자장치
은행장치
전자화폐후분(C')
및 r에 대한
이산대수형서명(Σ)
생성
S401
C'Σ,Certu,Pu 전송
S402
인증서(Certu) 및
서명(Σ)확인
S403
서명된
전자화폐(C)발행
S404
C 전송
S405
전자화폐(C)
유효성인증
S406
전자화폐정보(C,r)
저장
S407

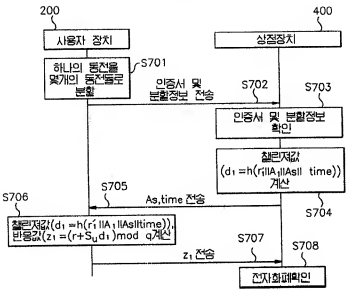
도면 5


200
400
사용자 장치
상점장치
c,Certu,Pu 전송
S501
인증서(Certu)확인
S502
챌린지값(d=h(Asiltimellc))계산
S503
As,time 전송
S504
챌린지값(d=h(Asiltimellc))및
반응값z=(r+Sud)mod q계산
S505
Z 전송
S506
전자화폐의
유효성확인
S507

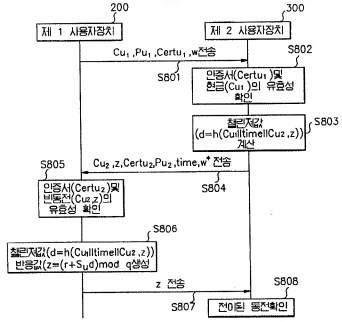
도면 6


400
100
상점장치
은행장치
c,Certu,Pu,d,time,As,z 전송
S601
S602
공개키(Pu)및 전자화폐(C)의
유효성 확인
S603
전자화폐(C)가
예치DB에 있는지
확인
있다
S605
없다
S604
인증기관 장치의
도움을 받아 이중
사용자 추적
상점장치의 계좌에
금액증가

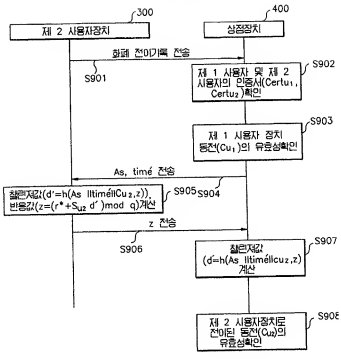
도면 7


200
400
사용자 장치
상점장치
S701
하나의 동전을 몇개의 동전들로 분할
인증서 및 분할정보 전송
S702
S703
인증서 및 분할정보 확인
챌린지값 (d1 =h(r‖IA1‖As‖ time)) 계산
S705
S706
As,time 전송
S704
챌린지값(d1 =h(r‖IA1‖As‖time)), 반응값(z1 =(r+SUd1)mod q계산
S707
S708
z1 전송
전자화폐확인

도면 8


200
300
제 1 사용자장치
제 2 사용자장치
Cu1 ,Pu1 ,Certu1 ,w전송
S802
S801
인증서(Certu1)및 한금(cu1)의 유효성 확인
챌린지값 (d=h(Cu‖time‖Cuz ,z)) 계산
S803
S805
Cu2 ,z,Certu2,Pu2 ,time,w' 전송
S804
인증서(Certu2)및 반독전(Cuz,z)의 유효성 확인
S806
챌린지값(d=h(Cu‖time‖Cuz ,z)) 반응값(z=(r+SUd)mod q생성
z 전송
S808
S807
전이된 동전확인

도면 9


300
제 2 사용자장치
400
상점장치
화폐 전이기록 전송
S901
제 1 사용자 및 제 2 사용자의 인증서(Certu1, Certu2)확인
S902
제 1 사용자 장치 동전(Cu1)의 유효성확인
S903
As, timé 전송
챌린지값(d'=h(As IltiméllCuz,z)), 반응값(z=(r*+Su2 d')mod q)계산
S905
S904
z 전송
S906
챌린지값 (d=h(As IltiméllCuz,z) 계산
S907
제 2 사용자장치로 전이된 동전(Cu2)의 유효성확인
S908